比特币

一个虚幻而真实的金融世界

李钧　长铗　等◎著

比特币

一个虚幻而真实的金融世界

李钧　长铗　等○著

中信出版社 · CHINA CITIC PRESS · 北京 ·

图书在版编目（CIP）数据

比特币 / 李钧，长铗等著. —北京：中信出版社，2014.1
ISBN 978-7-5086-4300-7
I. 比… II. ①李… ②长… III. 电子货币-研究 IV. F830.46
中国版本图书馆CIP数据核字（2013）第250196号

比特币

著　　者：李　钧　长　铗　李耀东　喻　峰　蔡卓斯　宋欢平　袁　维
策划推广：中信出版社（China CITIC Press）
出版发行：中信出版集团股份有限公司
（北京市朝阳区惠新东街甲4号富盛大厦2座　邮编　100029）
（CITIC Publishing Group）
承 印 者：北京通州皇家印刷厂
开　　本：787mm×1092mm　1/16　　印　　张：17　　字　　数：235千字
版　　次：2014年1月第1版　　印　　次：2014年1月第1次印刷
广告经营许可证：京朝工商广字第8087号
书　　号：ISBN 978-7-5086-4300-7 / F · 3047
定　　价：39.00元

推荐序1
比特币：预示未来货币形态和体系的实验

在过去的三四年间，我在世界的不少地方，向不同的朋友和学生讲比特币的原理和意义，和者甚寡。后来，我在北京见到李钧，得知他和他的朋友们撰写出中国第一本关于比特币的专著，与此同时，他们还是比特币的发掘者和拥有者。同时为这本书写序的李笑来就是比特币的成功实践者。对此，我由衷高兴。但是，我对于比特币的理解和肯定主要基于书本和文字，并不是比特币的实践者，也不拥有比特币，更没有用比特币生活过。所以，我更多的是从货币理论和货币历史的视角，讨论我对比特币的认知，难免有局限性。

（一）

2008年年末，源自美国的金融危机已经演变为世界金融危机，形成全球性恐慌，很多国家做出了过激反应。同时，现存的世界货币金融体系，以及对这一体系有至关重要影响的国际货币基金组织遭受普遍质疑。很多经济学家预测此次金融危机可能超过20世纪30年代的大危机。

就在这一年的 11 月，一篇署名中本聪（Satoshi Nakamoto）的研究报告“Bitcoin: A Peer-to Peer Electronic Cash System”发表。不到两个月，即 2009 年 1 月 3 日，经中本聪对其提出的比特币理论系统的实际运行，即所谓的“挖掘”过程，第一个比特币的区块横空出世，其中包含 50 枚比特币。

世界金融危机和比特币诞生在时间上的巧合，并不意味着两者存在直接相关性。但是，在世界金融危机和比特币诞生这两个孤立事件背后，却有着强烈的历史逻辑关系。

2008 年的世界金融危机，使得人们全面反思当代各国的货币体系，对各国的货币政策提出强烈批评，美元和美国货币政策则是众矢之的。有相当多的学者、政治家和企业家认识到：当代的世界货币体系，说到底，是各国法币的集合。只是在这个法币的集合中，美元是中心法币，扮演了法币的法币的角色。毫无疑义，美元对世界货币体系的衰变责任最大，但是，其他货币也不是没有问题。只有突破现行的世界货币体系，方可走出困境。问题是，目前为止没有更好的方案。最终，各国政府应对此次金融危机的基本手段大体是货币供给的量化宽松政策，扩大政府投资并强化对经济的影响力，其结果是推动了全球范围内新一轮的通货膨胀。恰恰是在这样的历史节点上，比特币提供了克服法币先天缺陷的一种崭新思路和选择。

（二）

法币的先天缺陷，说到底就是两条：第一，法币为政府所垄断，国家

是垄断货币发行的主体。法币是通过国家权力迫使民众接受和执行的一份合同；第二，因为国家通过中央银行决定法币发行数量，其本质是不稳定的。特别是19世纪70年代之后，随着美元与黄金脱轨，各国法币都转变成没有含金量的纯粹纸币，阻碍法币发行数量持续增长的最后制度和机制不复存在，法币贬值，或者说通货膨胀成为完全不可避免的事。从这个意义上说，哈耶克认为，“历史基本上就是政府制造通货膨胀的过程。”

现行的货币制度的后果是显而易见的。一方面，通货膨胀是国家收入的基本保障：“通货膨胀一直是一种有吸引力的可供选择的收入来源，因为事实上不用任何人投票表决，政府就可以利用它征收赋税，用凯恩斯的话来说，‘它是以一种无人能弄明白的方式做到这一点的。’”[①]另一方面，民众所创造的财富最终需要通过法币的形式显现，通货膨胀导致民众财富不断缩水。遗憾的是，长期以来，公众已经认定货币必须由某个最初的创造者创造，而国家就是创造者，是国家赋予货币的价值。货币天生就是政府的法币，法币就是货币的唯一存在形态。人们为国家垄断及其创造的货币付出了看不到尽头的代价，被货币奴役，逆来顺受。因为，在民众面前，并不存在可以替代政府法币的其他货币选择。

对此，哈耶克不以为然。1976年，已经77岁的哈耶克完成了《货币非国家化》一书。该书序言的开头是亚当·斯密在《国富论》里面的一段话：“我相信，世界各国的君主，都是贪婪不公的。他们欺骗臣民，把货币最初

① 弗里德曼，货币的祸害，商务印书馆，2007年，第242页。

所含金属的真实成分，次第削减。”该书的中心思想就是，除非各国政府不再拥有对货币创造的垄断权力，否则永远无法实现价格稳定。哈耶克的理想是：在一个国家，发行具有明显差异的，并由不同货币单位构成的货币，包括让私人货币流通，并实现不同货币之间的竞争。只有这样，所有的货币发行单位才会紧缩其货币发行量，以避免因货币不断贬值而最终被淘汰的命运。为此，哈耶克提出了详尽的货币非国家化的方案。

历史常常出现严重的不公正。《货币非国家化》的出版并没有产生实质性影响。哈耶克的理念被讥笑为政治上没有可能，技术上不可行。人们的思想局限在如何改进，而不是终结政府对货币垄断的体制。即使是激烈批评通货膨胀和现代货币体系的弗里德曼也认为哈耶克的希望无法实现：能够提供购买力的私人货币，是不可能驱逐政府发行的货币的。也就是说，只能在法币不可替代的前提下，通过控制法币发行数量，抑制通货膨胀。这就是货币主义。

无疑，在思想理念方面，弗里德曼的货币主义比起哈耶克的货币思想，是一种倒退，虽然是比较温和的倒退。

（三）

尽管我们无法得知，中本聪在设计比特币的时候，是否有实现哈耶克理念的动机或者潜意识。但是，事实是在哈耶克的货币非国家化的思想早已为人们淡忘的 42 年之后，中本聪所开创的比特币竟然证明了哈耶克货币理念是可以实现的。

第一，比特币天生独立于任何国家、任何政府、任何央行、任何企业。

第二，比特币是开源货币，是在P2P（点对点网络）中完成解码运算后奖励给运算者（即矿工）的礼物。单个节点会向全网广播交易，矿工收集交易信息打包成新数据块。

第三，比特币的创造过程是竞争性的，需要时间、能源和其他有形成本的投入。为保持数据块匀速生成，挖矿的人越多，挖矿难度就越高，成本呈现不断上升的趋势。

第四，比特币很可能是人类自从有货币以来的第一种可以避免不断贬值的货币。基于两个原因：比特币存在终极数量，其极限是2140年的2100万枚；比特币的P2P分布式特性与去中心化的设计结构，至少在理论上排除了任何机构操控比特币供给总量的可能性。

在货币理论历史中，有一个经过美国天文学家兼经济学家西蒙·纽科姆在19世纪末提出，再经欧文·费雪完善的著名方程式：MV=PT。其中，M是名义货币量，V是流通速度，P是价格指数，T是交易总量指数。但这个恒等式对于分析货币和价格的关系只具有理论和逻辑意义。在实际经济生活中，M的主要形式是政府发行的法币，其数量从来不可控制，而P必然是非稳定的。但是，如果M不再是不可控制的政府法币，而是比特币这样不会不断贬值的货币，那么，通货膨胀似乎是可以避免的。这个恒等式就具备了现实意义。

比特币价值的稳定和上升，意味着比特币的购买力的稳定和上升。比特币越来越值钱，用于购买物品和服务所需的比特币数量越来越少。也就

是说，比特币很可能有造成通货紧缩的能力，在一定程度上抵消全球通货膨胀的大势。

（四）

如果说，比特币的创造思想和方法是人类智慧的精妙显现，那么在过去短短的四五年内，比特币在全球范围被迅速传播，被人们接受和交易，规模膨胀，则无疑是货币金融领域的具有革命意义的事件，相信中本聪本人对此也是始料未及。

原因何在？答案是：比特币是财富创造和交换的创新。比特币的每笔交易既透明又匿名，每一个拥有网络客户端的人都可以查到全世界所有即时产生的比特币交易，却无须也无法得知这笔交易来自哪里，去向哪里，用作什么用途。比特币第一次从技术上提供了每一个个体自己创造的私有财产处于不可侵犯、不可冻结和不可追踪的状态。比特币的拥有者可以在完全以信任为基础的自由体系中，拥有和享用货币财富。或者说，比特币创造的是一个自己对自己负责、依靠信用运转的世界。货币主权要回归给个人，每个人有选择货币的权力，成为货币财富的主人。尤其值得注意的是，比特币生在互联网，用在互联网，加之个人间的匿名支付，使得任何政府至今无法对其交易实行征税。从根本上说，比特币是一种自由主义的生活方式。

比特币正在创建一个以比特币作为交换媒介的现实世界。比特币实现了虚拟世界和现实世界的结合，超越地域和产业部门的比特币“场”迅速形

成。不久前，各种媒体已经报道过：美国一对夫妇曾经尝试只依靠比特币生活。那似乎需要很大的勇气。而如今，比特币的应用范围从公益组织的捐款到日常应用，已经走进人们的生活。继德国宣布承认比特币的合法地位，会有更多国家加入，同时，全球接受比特币的商家也快速增加。

如果以为比特币代表的货币财富和交换体系仅仅存在于虚拟世界，将比特币简单归结于传统电子货币的一种，那是一种误解。比特币不同于传统的电子货币，因为任何传统的电子货币都要与政府的法币挂钩，至少依赖中心服务商，并没有自身的价值。而比特币与生俱有的就是其独立性，与任何政府发行的法币或中心服务商没有任何依存关系。所以，电子货币的本质必然是发散的，加剧传统货币供给总量的膨胀，而比特币的本性是收敛的，具有吸纳传统货币流通总量的能力，减少传统货币供给总量。此外，在物理意义上，比特币与一般电子货币也不同，其向周围扩散的过程不是无序的，而是有序的；流通密度不断扩展；不可能按时间顺序重复呈现比特币流通状态，交易不可逆。最值得注意的是，依附于政府和公司的传统电子货币是不可分割的，而比特币是可以分割的。当下，比特币的最小单位是小数点之后的 8 位数，如果需要，比特币可以分割为更小的单位。

相较于其他任何存在过和正在流通的货币，货币功能通过比特币得以充分实现。特别集中于以下 3 个方面：

第一，比特币更能实现货币作为交换媒介的功能，具有超越时空和超越主权的优势，应用版图遍布世界。

第二，比特币具有高度流动性的资产的功能，并成为当前全球升值最快的资产。

第三，比特币突破了传统资产负债表只能反映一个企业在某一特定时期全部资产、负债和所有者权益情况的局限，而比特币的账本不仅包括全部历史记录，而且是动态的，可以称得上是全息图像账本。

（五）

根据比特币过去三四年的表现，不得不承认比特币的爆发力。比特币正处于持续的“宇宙大爆炸”状态。2010 年 7 月 17 日，世界最大的比特币交易网站Mt.Gox成立，当时比特币的价格不到 0.05 美元。2013 年 11 月已经超过了数百美元，逼近上千美元，比特币价值的扩张不是以十、百、千为单位，而是以万为单位。

造成比特币规模扩张和价值上升的原因主要有两点：包括美元、欧元和人民币在内的贬值，与比特币的比价不断下降，导致比特币与其他法币的汇率不断攀升；由于个人投资者、金融公司和金融资本的加入，比特币的交易数量增加，推动比特币价格上涨。

问题是，在 2140 年之前，比特币的“大爆炸”状态，还会持续多久？比特币所代表的财富数量，何时可以进入相对稳定的阶段？对此，现在难以预测。但是，在比特币实现终极数量之前，始终会存在上涨空间是毋庸置疑的。根本而言，比特币的升值空间取决于比特币对世界实体经济和货币经济的影响

程度，以及比特币对世界生产总值的直接和间接贡献的程度。有人估算，如果比特币价格上涨到20 000美元一枚，比特币的规模接近世界经济规模的1%。

对于比特币的前途，有两种传统思维需要纠正。

第一，赋予比特币本身原本没有的意义。例如，比特币可能替代主权货币，甚至成为一种世界货币。比特币没有替代国家货币的使命，比特币的开源本质决定了它不会成为未来世界的唯一货币。

第二，将比特币的地位绝对化、神化，似乎不可替代。比特币的理念表明其一贯支持货币多元化，货币之间要竞争。近来，在比特币挖矿难度大幅提高的背景下，出现了类似比特币原理的若干新数字货币，如莱特币等，虽然各有不同的后发优势，依然无法形成挑战比特币、与比特币平等竞争的局势。比特币最值得肯定的是其开源本性、开放性和没有排他性。在理论上，不排除有一天会产生比比特币更完美的货币。

在过去的一年多时间里，中国成为比特币的重镇。自2013年夏季以来，比特币在中国的交易额已经超过世界交易额的40%，中国比特币市场的参与者不再仅仅是个人和小额资本，而是更多的商业公司和更大的资本。就在近日比特币价格疯涨的同时，有中国电商网站宣布，成功达成第一笔比特币订单。不同于之前的个人之间的私下交易，这是世界首例商业零售订单。中国成为比特币最大市场。在国家严格控制传统金融机构，银行业基本为国有银行垄断的情况下，比特币在中国的发展尤其需要深入解读。

有一点很值得提及：过去几年，中国一度盛行货币阴谋论和货币战争的说法，影响广泛。但是，至今还没有人将比特币的诞生视为一种阴谋，也没有人提出比特币会加剧政权货币之间的战争。[①]

（六）

在结束这篇序言的时候，我最希望表达的是：人类所经历过的货币国家化的历史，与货币非国家化的历史比较，实在是太短暂了。哈耶克主张的货币非国家化有足够的历史根据，却没有成为经济学界的主流，也不为民众所理解。在一些国家和地区，人们进行了诸如地区货币、社区货币的实验，却难以成势。比特币的出现，在唤起人们的货币非国家化的信念的同时，还提供了真实的实验。比特币证明了货币经济回归自由的可能性。

货币对历史进程的意义从来不可低估。比特币的历史意义，我们至今还难以充分认识。可惜，哈耶克和弗里德曼都已经过世，如果他们能够看到比特币，会做怎样的思考呢？

朱嘉明
经济学家

① 事实上，我过早庆幸了。就在我写这篇序言的当天，在网上看到了一种比特币阴谋论："神秘的背后往往暗藏阴谋，比特币恐怕就是一个巨大的阴谋……美国法院、参议院以及美联储之所以对比特币接连表现出极大的兴趣，一言以蔽之，就是希望借助互联网在线交易的巨大发展潜力，将比特币创建成一个主导全球在线支付的货币，进而在美元之外创建另一个由美国主导的世界货币。"（http://blog.sina.com.cn/s/blog_4a46559f0102e2oj.html）

推荐序2
比特币的天命

所有的事物和体系都有自己的空间和时间坐标。我们的世界因哲学、政治、宗教、文化和语言之限而分隔，却因交易的愿望而合为一体。这愿望是终极的人类社会契约，赋予我们学习、合作及竞争的共同动力。这样一个包含着和谐与纷争的无尽循环，创造了超出过往世代理解范围的现代奇迹。

但我们有这样一个问题：当今的全球金融体系拥有支配商业活动的权力。

古代世界关于饥荒、洪水和地震的恶兆，已经被金融崩溃、银行舞弊、政治对商业活动的管制和恶性通胀所替代。对于货币改革的支持者来说，中本聪的比特币仿佛一则预言，令我们振奋不已。2009 年 1 月 3 日，在比特币诞生的那一天，《泰晤士报》登载了《财政部长即将发起第二次银行救市计划》。

比特币不仅仅是一种货币，更代表着一种新的金融体系。它不再需要银行，也不需要刻意讨好中间人、机构或政府。它是一个超越地域和语言的体系，赋予世界以自由。而在此之前从没有人能将财富瞬间转移至世界任何一

个地方。我们借这个体系而联通，进而实现平等。

然而，如果没有一支“队伍”大声召唤，这个世界的金融体系难以回归和谐。他们必须向世人教授关于货币本身的社会契约，比如政府和原材料并不能创造价值；一种货币的价值永远取决于其能否有效行使以下职能：贮藏价值、单位计量以及在接受此种货币以交换产品和服务的人群中充当交易的手段。

他们必须教导大众如何通过比特币王国的考试。考试科目包括密码学、编程、点对点网络、奥地利学派经济学、企业家精神和比特币宣道精神，进而在人群中找到领袖。

这本书是你进入密码货币世界的开端。如果你希望通过考试，成为比特币世界的人才，那么你要做好准备，踏上一条危险与孤寂之路。但请相信，你不会独行。我们将会与你共渡这次旅程，抵达新的秩序与和谐。你我将成为彼此谦卑的引路人。

查尔斯·霍斯金森

比特币基金会教育委员会前主席

推荐序3
比特币：开源货币实验

比特币或许将是21世纪最优秀的发明之一，而在其向全球拓展的过程中，这本书将成为中国社区乃至全球比特币社区的引路人。作为中国第一本比特币领域的著作，其作者囊括了中文比特币社区里的7名重要成员，内容覆盖了比特币的历史、发展及未来等多个关键领域。

比特币不仅仅是一种货币，更是一项开源的去中心化运动，并且引起了更为广泛的讨论，例如货币本身所扮演的角色和所承担的使命，社会与政府之间的互动等。因此，对于个人来说，了解比特币的使命及大事年表是至关重要的。本书覆盖范围广泛，囊括了比特币发展过程中的各个里程碑事件，包括币值的大幅升跌、海盗党创始人理查德·法尔克维奇所做的工作、2013年加州圣何塞举行的比特币大会、加利福尼亚州政府与比特币基金会之间的官司纠纷、Mt.Gox交易所与美国政府间的沟通互动、比特币生态圈在德国的迅猛持续成长等。

而更深远的关注则落在了去中心化支付系统和交易所的未来上。比特币

是当今最优秀的加密货币，而其他的支付和交易体系，如莱特币也已崭露头角。这本书将目光投向了比特币和其他加密货币的未来，并同时将货币的历史和比特币的特有价值（这一价值远超其法币价格）纳入考量。

这本书将作为催化剂，围绕比特币这一主题，激发影响更为深远的对话。比特币及其对货币和社区的愿景使全球人民共同协作，相互分享。在一个小政府、自由市场以及如比特币生态圈这样的宣扬自由的环境里，要想成事，就必须对不同性别、不同信仰、不同文化甚至不同社会经济形态一视同仁。

比特币不仅仅是一种正在成长的电子货币，更是拥有巨大发展潜力的跨文化、无国界的货币，所有互联网用户都能使用。在全球各比特币群体正在迅速成长的今天，我期待中国比特币社区的进一步发展壮大。中国比特币社区的潜力巨大，而中国比特币社区的成功将是比特币长期成功的催化剂！我认为，这本书将进一步使中国及全球人民更深入地了解和支持比特币。让我们继续推动其在全球范围内的成长，使这一了不起的去中心化数字货币为人类所用，使其带来金融领域的进步。

伊莉莎白·浦劳熙

比特币基金会董事会成员

比特币基金会教育委员会成员

《比特币》杂志通讯主管

推荐4
比特币走向未来

做实验，有可能成功，也有可能失败。

实验失败了很正常，做实验的人继续改进就好。若一个人参与一个实验，而最终实验失败了，并不等同于那个人失败了。最终成功的人永远是这样的：一直在不断地做实验，失败了总结教训，成功了再接再厉。有史以来，一切进步都是由那些敢于正视失败的人创造的。

2011 年年初，《连线》杂志上刊登了一篇文章，讲述的是某种电子货币兑换美元的比率超过了 1 ： 1，而且该电子货币还是个开源软件！

如果说有人发布了一个开源电子货币系统，那只能被称为“试验”，可一旦这个东西真的开始流通，并且居然可以与美元相互兑换甚至比率超过 1 ： 1 的时候，它就应该升级为“实验”了。而时至 2013 年 4 月 1 日，当比特币兑美元超过 1 ： 100 的时候，在我看来，比特币已经进入了“实践”阶段。甚至连震惊一词都无法准确地表达我当时的感受。

我从网上下载了比特币发明者中本聪的论文，从头至尾反复研读了若

干遍。

在我一点点搞清楚的过程中，比特币的价格早就超过了3美元。我突然意识到这是一场越早参与就越划算的实验，因为它本身就是钱。时间就是比特币。于是，我卖掉了一部分当时被整个市场看好的苹果公司股票，在Mt.Gox上开了个账户，以每个平均6美元的价格，购入了2 100个比特币。

当时，我的想法非常简单，如果这场实验成功了，我自己将拥有一个经济规模的万分之一，那一定是很酷的事情！

一切来得太快，在我购入2 100个比特币之后两周之内，也就是2011年6月初前后，比特币价格上涨到每个22美元……我的1.2万美元已经变成了4万多美元！我相信所有商品的价格背后都有心理因素存在。我有点儿害怕了，害怕失去几天之内“赚到”的3万美元。于是，我开始着手一点一点地卖出。等我卖掉1 500个的时候，其价格已经达到每个28美元！也就是说，我只是点了点鼠标，手里就多出了3万美元，而且我还有600个比特币！

到那个时候，我自信对比特币的研究已经足够深入，而在深圳组装的一台矿机已经开始陆陆续续挖出一些比特币了。于是，我开始着手搭建自己的矿场。我甚至有更大的野心：搭建一个与Btcguild.com一样的矿池！

我开始在国内四处购买高端显卡，当时甚至买空了淘宝上的现货，最终从各处搜罗了46张显卡。在当时，20G的算力足够被称为“全亚洲最大的矿场”了。

可惜，最终的结果不尽如人意。现在回想，失败的原因在于，我做的事情并不是我自己可以全面掌控的事情。尽管我自己出得起钱，但在技术上，当时的我其实完全无能为力。出现任何事情，我都只能求助于他人。所以，当后来有人向我咨询比特币相关的创业项目时，我总是第一时间告诉对方："你最好认真回答自己一个问题，即这件事是不是你一个人就可以全部搞定的？"这是惨烈的失败之后得到的教训。

最终，"全亚洲最大的矿场"以挖出来100多个比特币告终，而当初投入的价值几十万的设备也只能以不到1/5的价格卖掉……

原本拥有这个经济规模万分之一的我，现在只剩下不到十万分之三……随着对比特币的更深入了解，那种失落感越发令我难以忍受。

我只好卖掉美股账号里的所有股票，然后投入到比特币交易之中。我"重操旧业"，开始做"我自己可以全部掌控的事情"。没有多久，我拥有的比特币数量开始没办法在交易所里直接交易，因为当时即便是全球最大的交易所Mt.Gox事实上也没有多少交易量。于是，我在比特币官方论坛上找到一些愿意做场外交易的人，从他们的手中买进卖出。到2012年年中，我已经没有多少美元可以用来购买比特币了，不过还好，我已经不再是那个"只要拥有万分之一就好"的人了……

再后来，我就不再像过去那样关注比特币了。重新开始关注已经是2013年元旦之后了。也正因为这样，我至少错过了两个好机会，即中本聪骰子（SatoshiDice）和烤猫（AsicMiner）上市。

2013 年 4 月 1 日，比特币价格冲破每个 100 美元。两年前，当我向身边的人说“坐等比特币涨到每个 100 美元”时，每个人的神色传递出的信息都是“你疯了吧”。可这一天终究还是来了，而新一轮的关注蜂拥而至。

这一轮关注热潮估计很快就会冷却下来，跟两年前比特币刚刚超过每个 1 美元时的情形如出一辙。两年后（也许用不了这么久），比特币还会冲破一个在此之前被认为是疯狂的价格，然后再引来一轮更大的关注吧。

至于现在，这场实验似乎还算成功。今天有越来越多的人参与这场“社会实践”。比特币像历史上的一切进步那样，在质疑声中成长，在指责谩骂中成熟。比特币也许是人类史上最令人敬畏的自生长系统。它不为任何人的意志所左右，它有自己的步伐，并用自己的节奏一步一步走向未来。

试验、实验、实践，我们共同前进……最终，真心希望我们能在有生之年见到比特币成为“实现”。

李笑来

资深比特币投资人

目录

01 初识比特币

比特币的诞生

上帝区块

从诞生那天起，比特币就注定是一个充满神奇色彩和颇多争议的事物。比特币里面包含了密码学、经济学、政治学、货币学、计算机技术等前沿的理论和技术。

从2013年年初开始，伴随着价格的疯狂增长，比特币频繁出现在各种科技和主流媒体的报道中，转眼成为时下热门的互联网金融领域最神秘的一部分。由于知识结构的局限性，很多人花了很长时间进行研究，但还是没有弄明白这到底是怎么一回事。很多人还在疑惑，比特币究竟是一场颠覆现有金融体系的伟大的互联网金融试验，还是一个由极客主导的庞氏骗局？

比特币这个概念最早由中本聪于2008年11月在一个隐秘密码学讨论小组中提出。当时，他贴出了一篇研究报告。随后，他又开发出最早的比特币发行、交易和账户管理系统。

随着2009年1月3日中本聪挖掘出第一个区块链（blockchain），最初的50个比特币宣告问世。至此，比特币这套系统可以算是真正诞生了。那时，又有谁能够想到，在短短几年时间内，比特币会被这么多人接受和喜欢，会以这么迅速的方式从极客圈走向社会大众，会以这么凶猛的价格增长方式来彰显自己与众不同的魅力呢？

自从互联网诞生以来，数字货币理念就一直是热门话题，但面临着如何解决伪造和重复支付等重大挑战。数字货币只是单纯的信息，怎样才能避免人们轻易地进行复制粘贴，然后随心所欲地进行支付呢？这一点至关重要，但解决起来困难重重。

在比特币出现之前，比较常见的解决办法是建立一个中央结算体系，对所有交易进行实时记账，同时确保人们使用过的电子货币不能再重复使用。这就需要一个有信誉的第三方机构来管理整个体系。日常生活中的银行系统都是采用这样的中央结算体系。

比特币却通过公开分布式账本的方法来避免重复支付，完全摒弃了需要第三方机构管理的架构。比特币所有的历史交易都通过块（blocks）的方式记录进账本，这个账本并不保存在某个中央服务器中，而是全网公开，保存在每个接入比特币网络的计算机上。

一条完整的交易指令被发出后，信息就在整个比特币网络内快速传播。网络节点开始计算该交易是否有效（即账户余额是否足够支付），并试图生成包含这笔交易信息的块。当累计有 6 个块包含该笔交易信息时，才被认为验证通过，正式确认交易成功。

供应机制

新的比特币是通过运行软件制造出来的，从表象上看，这种货币供应机制与金银等贵金属货币的供应机制有一定的相似之处，因此常被形象地称为“挖矿”，而挖矿的人则被称为“矿工”。也有人认为这个创造过程与游戏里面打金币非常相似，因此形象地称之为“打比特币”。

挖矿的本质就是争夺记账权。在比特币的世界里，大约每 10 分钟会在全网公开的账本上记录一个数据块，这个数据块里包含了这 10 分钟内全球被验证的所有交易。而确认这个数据块的权利是需要抢的，每抢到一个新的区块就允许获胜者向自己的账户增加一笔金额作为奖励。如果这 10 分钟内某个矿工没能抢到记账权（原则上每次只能有一个矿工抢到），他就等于白折腾了，重新进入下一轮争抢记账权的过程。

而争夺记账权的办法其实就是大家玩一个叫作哈希的密码学游戏，其具体算法是SHA-256（一种典型的安全散列算法）。

由于哈希计算结果的随机性，没有办法优化算法，只能从零开始一直往上运算，谁的运算能力强，谁就越有机会率先找到这个数字。因此，“发现”

新数据块的可能性是建立在个人计算能力与全网计算能力总和的比较之上的。

在比特币网络中，新币的生产速度是预先设定的。每个交易区块的生成时间保持在10分钟左右，最初每成功抢到一个块的奖励是50个比特币。区块链的规模每达到21万的整数倍（每4年会达到一次），成功抢到块获得的奖励便会减半：先从50个比特币减少至25个，再从25个减到12.5个。以此类推，大约到2140年整个系统将产生2 100万个比特币，达到事先设定的总量上限。之后比特币将不再增加，比特币矿工的收益将由转账手续费支付。

截至2013年9月2日，已被开发出来的比特币总量为1 164万个，考虑到早期的开采者没有意识到比特币的价值而造成的一些丢失，预计现在的比特币总量在600~800万个。

创始人是谁

比特币的创始人化名中本聪，但直到现在，他的真实身份依然扑朔迷离。有的只是无尽的猜测，甚至连是不是日本人，会不会是一个组织都难以考证。大家只知道，他肯定至少是一个超级优秀的算法工程师和程序员。

中本聪很少透露自己的信息，网上简介显示他在日本居住，但电子邮箱地址却来自德国的一个免费服务站点，谷歌上也搜索不到他的任何信息。

他之前在网上谈论的话题都只限于源代码技术讨论。2010年12月5日，在比特币使用者开始要求维基解密接受比特币捐赠后，他却在比特币论坛里发帖说：“这个项目需要逐步成长，这样软件才能在这个过程中不断增强。

我呼吁维基解密不要接受比特币，它还是一个萌芽阶段的小型测试社区。在这个阶段，如果不能妥善处理，只会毁了比特币。”

格林尼治时间 2010 年 12 月 12 日 6 点 22 分，就在他发帖争辩维基解密是否该接受比特币捐赠问题 7 天后，中本聪在论坛上发了最后一个帖子，帖子中谈到软件最新版本的几个无关紧要的细节。之后，他就从论坛消失了，他的邮件回复也变得不稳定，最后完全终止了。此后，中本聪只与少数几个人保持联系，作为后来比特币核心开发团队领导人的加文 · 安德烈森就是其中之一。2011 年 4 月 26 日，安德烈森告诉比特币开发团队的其他成员：“中本聪今天早上提议，在公开谈论比特币时，我们应尽量回避‘神秘创始人’这一话题。”随后，中本聪甚至连安德烈森的电子邮件都不再回复了。

神秘的中本聪彻底消失了，比特币爱好者对他的离开感到悲伤和不解。而中本聪的“孩子”——比特币——却以强大的生命力茁壮成长。

为了纪念他，有人开发了一种以比特币作为投注筹码的博彩小游戏，即中本聪骰子。这个游戏可以让玩家选择不同的赢面概率下注，完全随机，无法作弊，是比特币爱好者热衷的小游戏。2013 年 7 月，这个小游戏被一位神秘买家以 126 315 个比特币的价格（当时价值 1 150 万美元）收入囊中，成为比特币行业第一笔大额收购案例。

对中本聪的猜测和遐想是比特币爱好者颇感兴趣的话题之一，这不仅增强了比特币的神秘感，而且给阴谋论者提供了很多素材。

望月新一就是中本聪吗?

关于中本聪，有人怀疑这是由4家知名科技公司名字拼凑起来的，即三星（Samsung）、东芝（Toshiba）、中道（Nakamichi）和摩托罗拉（Motorola）。有人怀疑他的国籍，因为他的英语太地道了，简直毫无瑕疵。还有人怀疑这是有着某种未知目的的神秘组织，可能是谷歌甚至是美国国家安全局的团队。

2013年5月，计算机科学家、“超文本”概念的创造者泰德·尼尔森在美国知名在线视频网站YouTube上爆料，中本聪的真实身份是日本京都大学教授望月新一，瞬间引起轰动。不过他未能提供任何证据，只是根据一些迹象推断而已。视频中，尼尔森对望月新一极尽溢美之词，称他为伟大的经济学家、社会学家和计算机学家，甚至认为他应该因为比特币而获得诺贝尔经济学奖。

在数学领域，望月新一可谓大名鼎鼎：他16岁进入美国普林斯顿大学读本科，23岁获得数学博士学位。

2012年8月，对数学史上最富有传奇色彩的未解猜想——ABC猜想独立思考了20年后，望月新一在数学系主页上贴出了4篇总长度达512页的艰深推理文章，宣称自己解决了这一

猜想。由于文章内容太过艰涩，至今无人能够看懂。哈佛大学曾经邀请他去美国讲课，他仅回了一句“我的东西没办法给你们讲懂”就没下文了。

这样神奇的人物与比特币的特性着实吻合，因此尽管没有明显的证据，这一猜测也激发了热烈的讨论和验证。有很多人表示惊讶与兴奋，但更多人还是怀疑这种猜测的正确性：望月新一的确是一名出色的数学家，但怎么可能开发出这样一个势必对现实世界产生重大影响的货币系统呢？

现在看来，比特币的发明者中本聪的真实身份可能会一直是个谜。

如何获得比特币

刚接触到比特币的人都对它能兑换金钱表示很诧异，进而会寻求获得比特币的途径。一般来说，获得比特币的方法有 3 种：开动挖矿机挖掘、从交易平台买入、用产品和服务换取。通常情况下，比特币新手都会对挖矿比较感兴趣。

挖矿

比特币是通过运行复杂程序算法得来的，目前每天会产生 3 600 个新币。从理论上说，任何人都可以通过下载、运行软件来制造比特币。但事实上，

随着比特币的发展，矿机装备竞赛愈演愈烈，挖掘比特币的难度已非常大，需要拥有极高的算力才能勉强开采到。

根据比特币的供应机制，每个人能够挖到的比特币数量与其挖矿设备的算力占比特币全网算力总和的比例成正比。在早期参与者较少的时候，挖矿非常简单。据最早和中本聪合作的哈尔·芬尼回忆，他当时就开着个人电脑，几个星期就轻松地获得了几千个比特币。而随着矿机的大规模投入使用，截至2013年9月2日，全网算力已达到惊人的700THash/s（3个月前仅为100THash/s），而且快速增长的趋势还在延续。难度的增长在保障了比特币安全的同时也使得新币的获取异常困难。

以目前主流的算力为66GH/s的阿瓦隆（Avalon）矿机为例，如果超频到70GH/s，每天能够挖到的比特币也仅仅为0.36个而已，而且这个数量还在随难度的提升而迅速减少。

如果你试图用普通家用电脑挖掘，那么比特币将几乎永远不属于你，甚至会出现你花上几年时间却一个都挖不到的情况，白白浪费电费和人力成本。

买入

另一个获得比特币的方法是通过交易平台用法定货币（以下简称“法币”）来购买。交易平台颇多，较大的有日本的Mt.Gox、俄罗斯的BTC-e、中国的BTCChina，以及最近交易量稳坐第二把交易的Bitstamp。

比特币与法币的兑换汇率完全由市场决定，而且是7×24小时不间断交

易，不设涨跌幅限制。

由于现在比特币总市值并不大，容易被庄家操控，使得价格经常出现暴涨暴跌、反复无常的现象。它可以在一片质疑声中 3 年内猛涨上千倍，也可以在很多人都认为这就是未来货币雏形的时候，一周暴跌 80%。

交易平台是比特币产业链中相对比较容易受到攻击的对象，也曾经多次出现交易平台遭黑客攻击而丢币甚至被迫关闭的情况。比特币价格暴跌时，交易平台出问题的概率更高。所以，如果你对比特币的未来充满信心且长期看好，那么买入比特币后，建议提现到自己的离线钱包保存。

换取

不论你从事哪种行业，只要对比特币感兴趣，并且看好比特币的增长潜力，你就可以用你的产品或服务换取比特币。

上海的“巴别塔自由主义研究社”可算是一个用产品换币的典型代表。这本是一个以学习、实践和传播奥地利经济学派知识和理念为目标的社团，是哈耶克货币非国家化理念的忠实追随者，很自然地成了比特币的坚定支持者和推广者。

他们不仅以比特币拍卖的方式销售签名书，将销售所得捐给李笑来为雅安地震募捐比特币的项目，还印制了哈耶克文化衫，以支持比特币支付的方式进行销售。这些活动都获得了不错的反响，在传播哈耶克理论的同时也获得了一些收入。

虽然从比特币能够自由兑换美元那一天开始，它就已经和全世界几乎所有的商品建立了联系，但只有比特币直接进入交换商品和服务的流通领域才算是真正实现了价值，这些活动对比特币的发展具有长远意义。

比特币能购买什么

比特币的接受度

如果说比特币是货币，那么大家一定非常关心它能够购买什么东西。现在的答案是，由于全世界接受比特币的人越来越多，他们愿意接受比特币作为支付手段，所以比特币能够买到的产品和服务已非常多。

当然，在不同的国家和地区，其认可度并不相同：在欧洲国家的认可度最高，例如在芬兰和德国，即使只有比特币，你也可以轻松生活；但在中国，你的生活可能会相对困难。

随着认同比特币的人数的急剧增加，很多创业公司甚至主流网站已经开始支持比特币支付。这些公司的认同对于比特币是一种很好的推广和宣传，而比特币拥有者对这些公司也会比较慷慨，支持和捐赠都不在话下。全球比特币爱好者超过百万人，已是一个不容忽视的群体。善于想象的比特币铁杆粉丝甚至已在尝试建立仅支持比特币支付的实体社区了。

《福布斯》杂志的编辑刚刚用比特币生活了一周，美国犹他州的一对新婚夫妇决定使用比特币度过新婚后的 90 天，包括购买日常用品、为车加油、

支付租金等。他们建立了Life On Bitcoin（比特币生活）主页，用视频、图片和文字实时记录了整个过程。迄今为止，他们通过众筹网站Kickstarter和该主页共募集到570个比特币和72 995美元（截至2013年9月2日）。

可购买的物品

互联网网站和服务提供商对比特币的接受程度最高，例如，著名博客软件开发商WordPress和音乐、电影、软件目录网站BitTorrent分别于2012年11月和2013年4月宣布接受比特币捐赠；专注于用户生成内容的社交新闻和娱乐网站Reddit于2013年2月开始接受用户使用比特币购买Reddit的金牌服务；免费社交网站OkCupid从2013年4月开始接受用户使用比特币购买其特色服务。

2013年4月上线比特币时尚商店的Bitfash（Bitcoin Fashion Store）成为全球首个支持比特币的时装网站，用户在上面可以直接购买到Zara（西班牙服装品牌）、Forever 21（美国服装品牌）和Mr. Porter（英国著名线上男装精品店）的产品，并陆续有其他时尚品牌加入。迄今为止，国内支付领域的巨头支付宝还没有公布支持比特币的官方计划，但有部分淘宝店家不甘寂寞，宣布接受比特币支付。

在实体商店方面，也有一些商家接受比特币。比如创业咖啡馆和孵化基地“车库咖啡”就在国内率先支持比特币付款。如果你关心比特币社区的新闻可以发现，已经出现好几例愿意接收特币付款，出售其房产和汽车的案例。当然这些都只是少数个例，目前还没有大规模支持比特币支付的地产开

发商和汽车销售商。

支付应用扩展

成立于2011年5月的BitPay，总部设在奥兰多，是一家专门提供比特币支付方案的创业公司，有人把它比作比特币领域的支付宝。截至2013年9月，已经有7 500多家商户在使用其服务了。

由于Bitpay的存在，商家可以不需要直接接受比特币，客户支付的比特币可被自动兑换为法币并支付给商家，所以商家更加容易接受这种付款方式。另外，BitPay能够降低互联网付款的成本和风险，使得相同商品在BitPay上的价格要比竞争商家便宜1%~2%，因此能够获得更多人的认可。比特币的发展，从表面看来是市值的增加和财富的积累，但本质上一定是认可比特币理念的人口的增加。只有比特币越来越多地在某些方面承担货币功能，它才算是慢慢成熟了。

在比特币还不被很多人认可的时候，站出来认可和支持它是需要勇气的，也需要承受很多误解和偏见。请记住这些敢于站出来的企业和个人，不论他们是先驱还是先烈，至少他们曾经为自由货币的理想努力过。

支付的便利性

随着比特币社区的逐渐成熟和价格的阶段性稳定，比特币在小额跨境支付上的优越性正日益凸显。传统银行的国际汇款收费过高且不方便，而

比特币正好可以满足这方面的需求。一般认为，随着比特币市值的增加，价格的稳定性应该也会逐渐呈现出来，那么比特币极有可能成为一种稳定性强、流通性好的天然国际货币。从实用性角度出发，其需求和发展潜力也将是巨大的。

对于本地化的小额支付来说，手机客户端操作简单，便于顾客进行移动支付。口碑比较好的电子钱包包括Bitcoin-QT客户端、Coinbase（比特币支付服务公司币库）客户端以及Blockchain（提供比特币钱包服务的网站）客户端等。

Bitcoin-QT客户端界面非常简单，包含的内容有：钱包地址和二维码、余额、交易记录等。使用客户端可以很方便地支付或收款。

需要注意的是，Bitcoin-QT钱包和真实的钱包是一样的，手机一旦丢失，也就意味着钱包丢失，钱包里的钱是无法找回的。它不像有中央处理系统的银行，可以挂失并补办新卡。

而Coinbase客户端和Blockchain客户端实际上是在线钱包，登录账号后可以与电脑同步。即使不小心把手机丢了，还可以用新手机登录，只要不被盗号，账户里面的钱还是存在的。

比特币重要事件

瑞典海盗党创始人豪赌比特币

成立于2006年1月的海盗党目前是瑞典的第三大党，拥有议会席位，

被民间称为网络盗版党。该党号召民众投票支持网络自由下载合法化，而且抵制版权保护。

理查德 · 法尔克维奇是海盗党的创始人。2011 年 5 月，他撰写的一篇《为什么我把我的积蓄都换成了比特币》的博文引起了轰动。在博文里，他写道：过去的几天里，我做了很多关于比特币的思考，最后我决定把我所有的积蓄和所有我能借到的钱都投到比特币里面。

他做出这个决定时，比特币的价格大约为每个 8 美元，两年后的今天，每个已经超过 100 美元，以美元计价的财富增长超过 10 倍。

他当时给出了 3 个理由：

第一，在过去的 14 个月里，比特币对美元的汇率增加了 1 000 倍。目前还没有迹象表明，它将停止或已经饱和。

第二，比特币的使用不需要经过任何官方机构的同意，所以不需要向第三方支付交易费用，没有任何烦琐的手续。

第三，根据数学计算，在未来的几年内它的价值还会至少有 1 000 倍的增加。

年度比特币大会

2013 年 5 月 17 日，由比特币基金会组织，在美国加利福尼亚州（以下简称“加州”）圣何塞市举办了以“未来的支付方式”为主题的比特币 2013 大型会议，1 000 多名比特币发烧友、开发人员、企业家、风投家共聚一堂，

描绘这种虚拟货币的未来。会议由刚获得了500万美元风投资金的Coinbase赞助。

虽然1 000人规模的会议不算显眼，但头顶比特币的光环还是吸引了不少目光。现场到处都是发布比特币交易平台的创业企业、想要扩大比特币平台的软件开发商以及寻求投资标的的投资人。

比特币基金会的主席彼得·维斯塞内斯表示，目前基金会只有两名全职人员，计划在华盛顿聘请一名律师，负责与政治人物交流，希望能够早日摆脱监管困境，使比特币快速发展。基金会还在创建国际章程，以促进比特币在海外的扩张。

加州对比特币基金会的禁止令

在加州举办的比特币会议刚结束，政府就开始干涉了。6月24日，美国加州金融管理部门向比特币基金会发出终止信，认为基金会在未获政府授权的情况下进行了非法金融活动。根据加州法律，如果基金会不遵守政府发出的终止信，将面临每天或者每一笔交易1 000~2 500美元的罚款，如果被起诉，其创始人及管理者还可能会面临牢狱之灾。

比特币基金会的律师J·达克斯·汉森马上做出了回应，称比特币基金会是一个非营利组织，本身并不向用户出售比特币，也不参与比特币汇兑，根本没有从事货币金融业务。另外，比特币基金会办公室设在西雅图，并不在加州的管辖范围内。

Mt.Gox登记寻求合法经营

比特币的复杂属性使得每个国家对它的界定都存在分歧：德国联邦金融监管局将其定义为商品；美国金融犯罪执法网络（FinCEN）将其定义为去中心化货币，日本金融厅则认为它不是金融工具。

作为全球最大的比特币交易平台，日本公司Mt.Gox一度占据全球比特币70%的交易量，注册用户目前已超过50万。它一直在谋求交易的合法性以便扩大比特币的支付范围。

2011年夏天，法国工商银行曾经关闭了Mt.Gox的银行账户，理由是Mt.Gox公司不是银行，经营比特币这种电子货币是非法的。Mt.Gox提起上诉，由于法院不能认定比特币的性质，所以Mt.Gox得以继续在法国开展业务。

从2013年5月底开始，Mt.Gox就要求用户在提取美元时需验证身份。为了防止洗钱，Mt.Gox将非认证用户每天的交易额度设定为1 000美元，而提交登记信息的可以将额度提升至1万美元。

因为没有以正确方式注册，美国国土安全部在5月份冻结了Mt.Gox的两个银行账户，并责令在线及移动支付平台Dwolla停止为其提供转账服务（后来公布的法院文件显示，账上有290万美元，目前尚不清楚会怎么处置这笔资金）。6月20日，由于正在接受美国国土安全部的调查，Mt.Gox宣布暂停美元提现。

根据美国FinCEN 3月发布的监管条例，Mt.Gox从事货币兑换业务，必须向政府登记并申请货币服务（MSB）牌照。经过申请，Mt.Gox在2013年

6月28日获得了FinCEN的MSB牌照（31000029348132），终于实现了合法经营。

虽然实现了合法经营，但它迄今为止还没有找到合适的合作银行，导致平台上的美元难以流出，而比特币却可以自由流通，使一些人只能选择将账户上的美元转换成比特币。这种状况使得比特币在Mt.Gox的价格比其他平台高出10%左右。

德国的比特币生态

据德国《世界报》2013年6月27日报道，德国议会做出决定，德国自民党金融专家扎特提出的对比特币持有一年以上予以免税的议案得以通过。财政部决定将数字货币同传统的金融产品（股票、债券等）区别对待。持有一年以上，将不再对其征税。

7月11日，德国银行Fidor Bank AG与拥有7万用户的德国最大比特币交易站bitcoin.de达成合作。合作内容包括：Fidor Bank AG为bitcoin.de上的比特币交易提供责任伞保险，bitcoin.de客户可使用Fidor银行账户等。这是欧洲比特币行业首次与银行直接合作，将在德国联邦金融监管局登记备案后启动。

8月19日，德国财政部发表声明，承认比特币为一种“记账单位”。它既不是电子货币，也不是外币，更像是一种“私有货币”，可以用于“多边结算圈”。

作为比特币接受程度较高的欧洲国家之一，在很长一段时间内，德国政府在对数字货币的法律性质和税务处理上都存在一些争议。而此次在一个月之内，不仅确定税收处理方法，而且银行也开始正视比特币的资产价值，这对于比特币在德国乃至欧洲的推广和普及极具促进作用。

比特币在非洲被推广

在非洲，银行设施落后，资金流通不便，且手续费奇高。而基于手机的移动支付系统M-Pesa由于省去了人们的奔波之苦而在市场上取得了巨大成功，超过1/3的肯尼亚人和500万坦桑尼亚人都已经注册了M-Pesa。

目前，肯尼亚的一群退伍军人开发出了一种称为Kipochi的解决方案，可以使人们发送和接收比特币，并且可以实现与M-Pesa资产的自由转换。由于比特币不会贬值、流通方便、安全透明， Kipochi和M-Pesa在非洲的合作具有很大的发展空间。

知名比特币开发者杰夫 · 加尔兹克于2013年7月8日在Twitter（推特）上发布了一条信息："非洲会是一个可以受益于比特币的巨大的市场，比特币对非洲的好处甚至会比对富裕的西方国家更大。"

比特币基金会对话美国联邦政府

2013年8月27日，比特币基金会的成员与美国联邦调查局、美国国税局、美联储、美国货币监理署、联邦存款保险公司在华盛顿特区的美国财政

大楼中举行了闭门会议。比特币基金会的代表向上述联邦政府机构汇报了虚拟货币的本质，并就比特币的监管问题进行了商谈。美国的监管机构一致关注比特币的合法性问题，但之前基本都是在州政府层面进行沟通，这是比特币组织与联邦政府的首次会谈。

据美国卡托信息政策研究主任吉姆·哈珀透露，会上讨论了包括隐私、支付机构、监管以及如何更好发展在内的诸多问题。

基金会法规事务委员会主席桑托利认为：在比特币市场蓬勃发展的今天，明确的监管法律和监管部门不可或缺；比特币本身不需要监管，需要监管的是比特币的使用。

“丝绸之路”被查封

2013 年 10 月 2 日，美国联邦调查局（FBI）宣布逮捕年轻人罗斯·威廉姆斯·乌布利希。据信，乌布利希是“丝绸之路”网站站长。

“丝绸之路”网站上线于 2011 年 2 月，允许用户使用比特币进行匿名交易，还采用了一种叫做“洋葱路由”的技术，让追踪变得更加困难。这种“超级安全性”使得“丝绸之路”很快受到了某些人群的追捧，非法交易丛生，交易物品包括毒品、黑枪、信用卡资料、色情服务和黑客服务等。该网站对每一笔交易都征收 8%~15%的手续费，获利异常丰厚。

FBI彻底捣毁了该网站，并扣押了乌布利希的 2.6 万个比特币，时价约 360 万美元。后来又有消息称乌布利希尚拥有另外 60 万个比特币，其中有

14.4万个已经移交给FBI，另外48.9万个的最终归属尚不得而知。FBI查封“丝绸之路”的当天比特币价格下跌了15%左右，但是第二天就基本恢复正常。许多比特币玩家认为，FBI打击的是非法交易，并非比特币。像“丝绸之路”这样的非法网站被查封，实际上净化了比特币的交易环境。

世界首例比特币零售订单完成

2013年10月30日，国内企业果壳电子宣布开通比特币支付功能，果壳旗下GEAK Watch智能手表、GEAK Eye/Mars智能手机均可使用比特币购买。就在今年“双十一”期间，有国内用户真的用比特币在果壳电子官网购买了两块果壳智能手表，果壳电子也已为其发货。宣告了比特币的世界首例零售订单完成。当然，这更多的是一种极客精神的体现，比特币支付还有很长的路要走。

比特币的名人效应

创新的传播

传播学教授埃弗雷特·罗杰斯在他的专著《创新的扩散》中对创新的传播进行了全面阐述。他认为，创新（一个理论、一项实践或一个产品）过程伴随着不确定性，创新的实质是提供解决问题的新方案。但对于决策者来说，他并不清楚这个新方案在多大程度上优越于传统的解决方案。

在罗杰斯看来，在创新扩散的过程中，早期看似势单力薄的群体能够在人际传播中发挥很大的作用，他们率先接受和使用创新事物并甘愿为之冒险。这些人不仅对创新初期的种种不足有着较强的忍耐力，还能够对自身所处各个群体的意见领袖展开游说，使之接受乃至采用创新型产品。之后，创新又通过意见领袖们迅速向外扩散。这样一来，创新距离“起飞期”就越来越近。

持续创新的能力是人区别于动物的一个重要方面，人们通常会思考：如何将一个产品做到更好，如何将一种制度设计得更完美，如何将一套理念理解得更加透彻。同时，创新是多方向的，很难预先知道哪个方向是正确的。对于个体来说，创新方向的错误会带来失败，但对于群体来说，从多个方向中选择最佳的那个一定是有利的过程。

对于一种新兴事物，不论是产品还是观点，一般都会有一定的门槛，比如技术或理解力。通常只有少数人会率先理解、尝试和使用，他们属于试错者、创新者，但也完全有可能走在错误的道路上。

如果他们的创新的确能够推动社会进步，就能够说服早期跟风者使用产品或者接受理念，而接受者会逐渐成为主流，甚至连非常排斥的人也被迫跟进，其出发点可能仅仅是防止被淘汰。

对创新的接受程度与个人的学识、阅历有关。由于个体差异，同一种创新产品在不同的人眼里可能是截然不同的东西。比特币的创新在很多程序员看来，是那么显而易见，简直就是数学接管世界的起点；而在有些人眼里，

这只是毫无价值的浪费电力的传销产物。

任何一种观点都有自己的市场，正如罗杰斯在其专著中提到的，会有“劝服、决策和证实的过程”。创新只有被大众接受，才可能成为更广泛意义上的社会产品。在这个传播过程中，在人群达到一定数量的时候，通常会有一个引爆点，用户的指数级增长会是一个典型标志。

对于比特币来说，如果你真的不太懂加密算法、硬件知识、货币理论、金融趋势，除了可以从《创新的扩散》、《失控》、《货币的非国家化》、《货币生产的伦理》、《美国货币史》这样经典的著作中汲取营养外，还有一种很好的方式：找出比特币领域的创新者和公认的精英，了解他们的观点。这对于你判断比特币这一创新的未来发展趋势有很大的借鉴意义。

名人眼中的比特币

比特币价格在 3 个月内上涨十几倍的疯狂态势吸引了无数人的眼球，科技、金融巨擘们都被媒体追着要求发表看法。其中有比特币的狂热爱好者，也有对比特币还缺乏足够了解的精英。他们的言论能够为我们提供参考。但需要提醒的是，资本市场是残酷的，所以不论这些精英怎么看，仅可以当作参考。要想看清比特币，还得靠自己。

/巴菲特、比尔 · 盖茨和查理 · 芒格/

作为久负盛名的投资大师，巴菲特对比特币的看法一定是很多人关心

的。在2013年5月的伯克希尔·哈撒韦公司股东大会上被问及如何看待比特币时，巴菲特表示："我们共有490亿美元的资金，但我们一分钱也没有投到比特币上。我对比特币成为一种通用货币一点儿信心都没有。"

几天后，美国福克斯电视台曾专门邀请巴菲特、比尔·盖茨和巴菲特的好搭档查理·芒格一起座谈，询问他们对比特币的看法。

查理·芒格心直口快："我觉得比特币就是能害死人的老鼠药，我虽然不懂，但我知道这玩意儿就是不靠谱。"

比尔·盖茨比较谨慎，他只是面带笑容地评价说："我觉得它是技术上的杰作，但它所涉及的领域应当让政府保持主导地位。"

巴菲特不置可否，只是说了一句："我不了解比特币，但我知道他们俩肯定有一个是对的。"

/卡马斯/

卡马斯是美国社交网站Facebook（脸谱网）的核心成员，曾长期担任副总裁，主管增长、移动与国际业务。他也曾经投资过诸多创业公司，目前正在运作着社区资本基金（TSCF）。

卡马斯在科技博客网站TechCrunch于2013年4月举行的2013TC Disrupt创业公司大会上说："我个人的风投资金中有比特币，我的基金中有比特币，我的私人账户中也有比特币……你现在谈论的这种东西是为未来三五年准备的好到难以置信的保值品。它就是黄金2.0，不是吗……我能用

比特币去做不在任何政府管辖范围之内的事情，比特币能在你想象到的任何地方使用……比特币很可能成为一种付款机制。”

/约翰 · 多纳霍/

eBay（易趣）首席执行官兼总裁约翰 · 多纳霍在接受美国CNBC（消费者新闻与商业频道）采访时称，比特币是“仍处在非常非常初期的颠覆性创新创意的另一个案例”。他认为比特币有趣，随着不同利益相关者的加入，它可能会找到出路。他在接受《华尔街日报》采访时说，“比特币是颠覆性的技术，我们正在仔细观察，可能有多种方式将它融入Paypal（贝宝）。”他还表示，对Paypal是否采用比特币不做任何承诺。

/保罗 · 布赫海特/

保罗 · 布赫海特是谷歌邮箱（Gmail）和广告联盟（AdSense）的创始人。2009 年，布赫海特创立的社交媒体创业公司Friendfeed被Facebook收购，他随公司加入Facebook，2010 离开后成为美国著名创投公司Y Combinator的合伙人。

2013 年 4 月 29 日，他在Twitter上发了条消息：“Bitcoin may be the TCP/IP of money.”（比特币有望成为金钱的基础协议。）从这条短短的消息中可以看出他把比特币置于何种高度，进而引发了很多讨论和猜测。

/阿尔伯特 · 温杰/

阿尔伯特 · 温杰是美国顶级风险投资机构USV（联合广场风投）的合伙人。USV曾经投资过Twitter、Tumblr（汤博乐）、Foursquare（社交定位网站）、Etsy（手工艺品在线集市）、Kickstarter和Shapeways（3D打印创业公司）等知名企业。USV现在也是投资虚拟货币创业公司的先锋，已投资了Coinbase。

他在个人博客上称，如果将来比特币的使用规模能够占据世界经济规模的1%，那么比特币的价格应该达到2 000美元/个。

/李笑来/

原新东方学校教师、原艾德睿智国际教育咨询合伙人、畅销书《把时间当作朋友》作者李笑来从2011年开始筹备显卡矿场，但以失败告终。之后，开始利用资本的力量低买高卖。在央视的采访节目中，他自称有6位数的比特币。2013年6月，他成功募集2 000万元人民币，创建了国内首只大型比特币基金Bitfund。

为了给100多个有限合伙人一个更好的交代，李笑来把教育咨询公司的股份送人了，连他在2013年年初创立的Knewone（新奇科技产品导购网站）也只留了少量股份。

他的观点非常直白："我反复强调，同样的东西放在那里，人们各自看到的是不相同的，至于他看到的是什么，完全取决于他过去的知识积累和他

的思考层次，仅此而已，所以很多争论是没有必要的。”

/保罗 · 克鲁格曼/

身为麻省理工学院经济学教授、诺贝尔经济学奖得主，2013 年 4 月，保罗 · 克鲁格曼在《纽约时报》网站上接连发表两篇文章——《亚当 · 斯密认为比特币很傻》和《反社会的网络》，批评比特币。其核心思想是耗费现实资源制造虚拟的比特币是愚蠢的，比特币的狂热追随者们不懂货币，严重误解了货币。他还引用萨缪尔森的观点，称货币是一种“社会发明”，无法超然于社会之外存在，而比特币试图把货币的价值从它所服务的社会中抽离。

社会属性带来的分歧

所有社会科学课题的研究和论述都很难得到统一的标准答案，通常是持不同观点的人尝试说服更多人接受自己的观点，进而使自己的观点成为主流。这样的例子非常多，比如死刑废除与否、同性恋婚姻的合法性、政府调控经济的手段等。

比特币的社会属性与技术属性一样重要，而且在成为通用货币的过程中，其社会属性会越来越强。在一定时间内，观点的分歧是必然的，也是无法改变的。而比特币支持者对比特币的理解、推广以及应用本身就是增加其社会价值的方法，也是帮助社会整体更准确地理解比特币、减少分歧、赢取共识的途径。

02 震撼世界的比特币

过山车行情

比特币诞生于2009年，最早是局限在小圈子里的极客玩物。在密码破译界以外的用户开始慢慢熟悉比特币后，它赢得了很多电子货币行业资深人士的赞许，但谁也没有想过可以用它来兑换真实世界的货币。早期的玩家基本都是本着分享开源软件项目的社区精神，投入运算能力，维护比特币社区的运转。

美国佛罗里达州程序设计员拉斯洛·豪涅茨一般被看作是第一个在现实世界使用比特币的人。2010年5月，他用1万个比特币换回了一张比萨连锁店棒约翰的比萨优惠券（当时价值25美元）。现在，1万个比特币的价值为100多万美元，足够在美国换一栋豪宅加一辆豪车。人们问他怎么看，他只是笑笑说，比萨味道不错，就是有点儿贵。

这份目前价值上百万美元的比萨是比特币在几年时间内价格飞涨的最好注脚。

第一次暴涨暴跌

2011 年 1 月，1 个比特币还不值 30 美分，但在随后的几个月里，它一路突破 1 美元、8 美元、20 美元， 2011 年 6 月 9 日达到 29.55 美元，半年时间涨幅约为 100 倍。

在一片叫好声中，一些令人不安的事情开始困扰比特币持有者。

2011 年 6 月中旬，一位名为Allinvain的用户称自己的 2.5 万个比特币（当时价值 50 多万美元）被盗。6 月 19 日，这个朝气蓬勃的网络金融试验遭受突如其来的重创，Mt.Gox 上出现了令人震惊的售价：一分钟内，比特币的交易价从每个 17 美元跌至每个 10 美元，几分钟后，价格降至每个 0.013 4 美元。最终，有 26.1 万个比特币以每个 1 美分的价格成交。30 分钟后，比特币价格又重新回到每个 13 美元。

Mt.Gox随即发表声明称，价格急剧波动是因为一个拥有很多比特币的账户被黑客攻破。该黑客在低价抛售的同时，又用另一个账号吃进。幸运的是，Mt.Gox有每天提现不超过 1 000 美元的限制，这名黑客最终只转走了价值 1 000 美元的比特币。

Mt.Gox 因此停业一周，之后虽然恢复了服务，但此事严重动摇了比特币爱好者的信心，并引发了一连串的负面报道，比特币的价格也随之一路走低。

价格暴跌使比特币在公众心目中的地位，一夜之间就从未来货币变成了

乌托邦式的笑话，但比特币的忠实粉丝依然坚持自己的信念，不论对中本聪本人还是对他建立的整个系统都是信心满满。

即便如此，比特币的价格还是一路狂跌，仅仅半年时间后的2011年11月，比特币的最低价格已降至每个2美元，相比6月份的最高价缩水90%以上。

第二次暴涨暴跌

经历了2011年的暴跌之后，比特币的总市值缩水为千万美元，从大众喜爱的投资品变回了极客圈的玩物，也逐渐消失在媒体的视野中。在整个2012年，比特币交易并不是非常活跃，媒体也鲜有大规模讨论，但价格却慢慢的从年初的2美元涨到了年底的10美元。

2012年年底发生的几件大事又重新触发了比特币的暴涨行情。从2013年2月开始的两个月里，价格上涨超过10倍。

/4年产量减半的时间点/

比特币历史上的第一个每天新币产量减半的日子终于到来了。根据每4年减半的设定，第一个4年的节点是2012年11月28日。在这之前，每10分钟产生的一个新的运算块（block）会奖励50个比特币，每天产生的新币总量为7 200个，而在此之后，每个运算块的奖励减为25个比特币，每天只能产生3 600个新币。

如果根据新币的生产成本判断其价值的话，那之后的生产成本就相当于

增加了一倍。即使根据简单的供求关系判断，在每天的供给量突然减半，而需求还在上升的情况下，价格也是会逐渐上升的。

/集成矿机的投入使用/

由于比特币挖矿有利可图，且根据其分配原则，运算能力就是分配权，因此逐渐有资本投入研发ASIC（专门用于挖矿运算的高效率集成电路）矿机。随着南瓜张阿瓦隆（Avalon）和烤猫矿机的成功研发与投产，比特币的挖矿难度急剧提升。

难度的提升意味着显卡矿工挖矿的收益将减少。如果以显卡挖矿为标准，相当于比特币的生产成本提高了。成本的上升给价格的上升提供了有力支撑。当然，这样的计算方法并不被很多人认同：一些人认为，在现在的挖矿装备中，显卡已经完全被淘汰，矿机虽然具有强大的运算能力，但生产成本并不高，市场价格的居高不下是由于技术垄断，也有人由此预测比特币将进入下跌通道。

/区块链分叉事件引发短暂恐慌/

2013 年 3 月 12 日，使用 0.8.0 版本客户端的比特币矿工创建了一个大区块，但该区块与之前的 0.7.0 版本客户端创造的区块不兼容，使用比特币新版本的矿工、商家、用户接受了这个区块，但旧版本的使用者选择了拒绝，并生成了自己独立的区块链，导致了区块链的分叉。这一问题致使比特币价

格当即下跌了 30%。

当然，问题解决得也很迅速。比特币基金会经过讨论，决定关闭比特币交易平台，并通知矿池退回旧版本并创建适合所有比特币版本的区块链。之后，旧版本与新版本的区块链产生速度相当，问题得以解决，比特币价格也迅速回弹。

由于是在一天之内解决了问题，并没有造成价格的大波动，绝大部分人甚至都没有觉察到危险，但很多真正了解比特币原理的网络工程师都把这次事件看成是真正威胁到比特币安全的大事件，认为这简直就是一次 51%攻击的预演。（所谓 51%攻击，之后会详细阐述。）

在此次区块链分叉事件中，比特币基金会迅速提出解决方案并付诸实践的做法广受好评。

/塞浦路斯事件推波助澜/

爆发于 2013 年 3 月的塞浦路斯银行危机凸显了货币背后国家信用背书的无力，成为映衬比特币价格飞涨的良好背景。

塞浦路斯借助自身离岸金融的发展模式，吸引了大量的海外存款，而其中又有大部分投资于希腊国债一类的收益高、风险大的海外资产。欧债危机爆发后，希腊国债的市值下跌以及部分违约使塞浦路斯的银行业遭遇巨额亏损，需要得到外部资金的援助，否则金融业将迅速瘫痪，且有可能退出欧元区。

塞浦路斯期望欧盟能够提供100亿欧元的纾困资金，欧洲央行同意拨付，但同时要求其自行筹集58亿欧元。

2013年3月16日，塞浦路斯政府为了得到这笔援助，同意向银行储户征收一次性存款税，10万欧元以上的存款税率为9.9%，10万欧元以下的存款税率为5.6%，但该方案于3月19日遭议会否决。

此后，塞浦路斯政府向俄罗斯求助未果，而欧洲央行于3月21日又向塞浦路斯政府发出最后通牒，要求其必须在3月25日前按照救助协议要求筹集资金。

最终，塞浦路斯与欧盟、欧洲央行和国际货币基金组织组成的“三驾马车”达成协议：关闭塞浦路斯第二大银行大众银行，该行10万欧元以下存款将转移至第一大银行塞浦路斯银行，10万欧元以上存款中超出10万欧元的部分，37.5%被转为塞浦路斯银行的股权，22.5%被冻结，剩下的40%被暂时冻结直至援助结束。

于是，人们疯狂地寻求资金出路。他们突然发现，比特币或许可以挽救其财富。随着比特币钱包下载量的突飞猛涨，比特币价格也一路走高。从3月下旬到4月10日，仅用了3周时间，比特币兑美元的价格就从65美元升至有史以来的最高值（266美元），增幅超过3倍。

/价格泡沫破裂/

2013年4月10日晚，比特币价格突然从每个266美元跌至每个105美

元，一天之内跌幅超过61%，并在之后的一星期之内一度跌至最低每个50美元。

对于很多刚刚通过大众媒体了解到比特币，看好并大量买入比特币的人而言，那一晚简直就是噩梦般的死亡之夜。由于比特币的24小时交易属性，很多人都是早上醒来时才发现价格已经下跌了40%。交易所被攻击没法登录，各种负面消息扑面而来，一夜之间，比特币的致富梦变成了负债泪。

这就是金融市场的残酷：由于市值小、7×24小时交易，比特币很容易成为资本操控的对象。

任何资本市场都会有庄家，一拥而上、一哄而散的散户往往是被宰割的对象。即使比特币的原理再完美，未来再美好，现在仍处在初期，发展过程中的大起大落一定会让很多人流泪退场。

/全球媒体轰炸/

比特币从2013年1月开始上涨，短短3个月内价格就增长了10倍以上，制造了巨大的财富效应，国内外媒体争相进行研究和报道。

科技媒体和大众媒体进行报道的深度和思考的层面是不一样的：科技媒体喜欢分析其内在机理，试图从原理上理解其内在价值；大众媒体则喜欢分析其社会效应，擅长从社会影响方面预测其增长潜力。从一定意义上讲多方位的媒体轰炸也是推动这轮价格大涨大跌的重要因素。

在这次疯狂的浪潮中，《福布斯》杂志的编辑卡什米里·希尔艰难地说

服别人接受比特币，用比特币满足衣食住行的需求。他依靠比特币生活了一周，并记录了每天的生活。从中我们可以看到，目前想单纯地依靠比特币生活仍非常艰难。

比特币价格的爆发式增长，也引起了国内媒体的跟进报道。新兴的科技媒体如Pingwest、36氪、虎嗅网、爱范儿、创见等通过原创或翻译资料对比特币进行剖析；第一财经、央视等大众媒体随后加入讨论阵营，对比特币做了一次全国范围的科普。

在价格飞涨的疯狂时期，媒体轰炸和价格泡沫互为因果，比特币价格的一路上升惊动了媒体，媒体报道又吸引了更多的参与者，进而加剧了泡沫。在价格稳定时期，媒体的参与能够让更多的人真正地学习和了解比特币的内涵和精髓。

第三次暴涨

经历4月的暴跌之后，比特币经过一个月的调整，逐渐恢复元气。到5月下旬，其价格一度攀升到130美元左右。6月上旬，受美国国土安全部冻结Mt.Gox美国银行账号和Mt.Gox寻求“合法化”的影响，价格又跌至70美元左右。此后，比特币的价格又开始持续上扬，10月2日的“丝绸之路”事件亦未能阻止其上涨趋势。10月23日，其价格一度超过230美元，而在11月初，比特币一度站上340美元的高位。

比特币的这一轮上涨，中国用户功不可没，据测算，国内比特币的交易

量已经位居全球第二，仅次于美国，甚至一度超越。10 月 23 日的价格暴涨普遍被归因于国内“大户”的进场。这轮涨势能持续多久，是否会被某种因素打断，是否会再度出现暴涨暴跌的轮回，有待后续观察。未来，FBI如何处置其缴获的比特币（尤其是假如FBI完全掌握了乌布利希剩余的 48.9 万个比特币，那么FBI拥有的比特币总数将占到已发行量的 5%以上），很有可能会对比特币价格产生重要影响。

价格的依据

比特币价格长线增长、短线忽上忽下的过山车行情令很多人惊诧不已。抓住了机会的人在欢呼一夜暴富，而高点买入的人则在后悔没能把握住时机；拿到首批集成矿机的矿工们享受着几十倍的收益；而集中出芯片后预订期货矿机的人很可能收不回成本。

矿工和比特币炒作者、投资者都会思考如下问题：比特币的合理价格到底是多少？其价格的支撑体系又在哪里？最后能不能形成一个稳定的价格？如果不能形成稳定的价格，它又如何成为充当一般等价物的货币呢？

我们通常用比特币新币的挖掘成本来衡量价格的合理性。根据矿机投入折旧以及挖矿电费和人力消耗，结合全网运算能力（挖矿难度）的发展预期，可以大概估算每个新币的生产成本。当然，这个成本在不断变化：一方面，随着矿机硬件技术的提升，单位运算能力矿机的生产成本和能耗都在降低；另一方面，随着挖矿设备的增加，单位运算能力能够挖掘到的比特币会

逐渐减少。整体来看，新比特币的挖掘成本在快速上升。

其实虚拟货币所有的价格都是心理价位。成本核算具有一定的参考依据，但实际的涨跌是成本与市场信息的综合产物，由于新币占总量的比重较小（每天新产生的 3 600 个相对于 1 100 万个的总量和每天 10 万个左右的交易量来说是微不足道的），其生产成本能够提供的价格支撑的更多的是象征意义。从中短期来看，利好和利空消息对比特币持有者的心理预期影响远大于生产成本，进而对价格产生较大影响。

每次暴涨暴跌都发生在热点事件出现、新闻媒体推波助澜、大批新手涌入的时候。可以想象，在全球货币贬值、通胀预期严重的大背景下，一种总量恒定的货币对于默默承受着货币贬值后果的普通民众来说具有多大的诱惑力。在各种利好条件的支撑下，群体无意识的非理性冲动推动着价格泡沫一路膨胀。当价格飙升到一定的高度时，势必会出现大单抛售情况，泡沫由此破裂，任何一条负面消息都可能成为暴跌的导火线。

许多人也认为价格暴涨暴跌是比特币发展过程中的必经阶段，每次泡沫破裂都是比特币老手从尚未理解价格形成机制的新手那里获得收益的机会。对于新手来说，这就是昂贵的学费。但随着社会对比特币的接受面越来越广，了解越来越深，其涨跌幅度可能会缩小。比特币发展越成熟，其价格就会越稳健。不管是芯片研发还是挖矿，都会有一个合理的收益率，门槛高的工作的收益率会相对较高，但已不能与早年夸张的数倍收益相提并论了。

比特币暴富神话终结的日子就是比特币成熟的日子。比特币逐渐走向社

会大众的过程是比特币逐渐分散的过程，也是价格逐渐平稳的过程。

政府怎么对待比特币

“货币的非国家化”学说

亚当·斯密在《国富论》中指出，根据自然的自由制度，政府应当承担3项职责：保护本国社会的安全（国防）；保护人民不受社会中其他成员的欺侮和压迫（司法）；建立和维持某些公共机关和公共工程（公共服务）。其中并没有提及货币的发行权。

货币是否可以引入竞争机制？货币的加速贬值使越来越多的人开始对凯恩斯的宏观调控理论产生警惕心理，即大政府对货币政策的调控是否合理合法。

不论是组织还是个人，都有自我膨胀和自我发展的需求，这对政府同样适用。如果没有一种合理的机制来制约，过度膨胀的政府会损害经济。

哈耶克在他的专著《货币的非国家化》中提到：“如果一种货币的发行量被一个机构刻意控制着，而这个机构的自私自利驱使它满足了其使用者的愿望，那么它就是一种最佳货币。”他的建议就是“废除中央银行制度，允许私人发行货币并自由竞争，在这个竞争过程中将会发现最好的货币”。哈耶克进行了数十年的逻辑思维试验，得出了允许私人发行货币进行竞争，最优、最稳定的货币自然会胜出的结论。

哈耶克即使再聪明，预见能力再高超，也肯定难以想象，在他去世后的20年里，互联网会得到这么迅速的发展，大量新概念不断涌现。在他诞辰110周年的2009年，比特币“呱呱坠地”；经过几年的发展，他的非国家化的货币理想正隐约实现，虽然和他设想的形式有些不同。

政府的态度

比特币发行的一个核心特点就是发行和交易的去中心化，但去中心化并不意味着不需要监管。比特币行业中的骗局屡屡发生，适当监管是发展过程中的必备要素。

政府对比特币的态度可能会极端矛盾：一方面，担心比特币的成功会影响政府对货币政策的控制力度，所以希望能够控制或限制其发展；另一方面，只要互联网存在，比特币就难以禁止，如果比特币最后在全世界范围内取得成功，现在的管制将会使本国国民付出巨额的代价。

由于互联网的发达以及政治理念的约束较少，比特币在欧洲和美国的接受程度相对较高，政府相关部门也制定了相应的条例予以规范和约束。

2012年10月，欧洲央行出台《虚拟货币报告》,对比特币做了专门介绍，并表达了对其安全性以及可能被用于非法目的的担心。

2013年3月18日，美国FinCEN出台了针对虚拟货币的监管条例。条例中明确了用户、交易商和管理员的定义：用户指使用虚拟货币购买商品或服务的人；交易商是专门从事虚拟货币与真实货币、基金或其他货币兑换的人；

管理员是专门从事虚拟货币发行或拥有虚拟货币回收权力的人。管理员和交易商从事的是货币服务业务，需要以“货币转移者”身份接受相关的登记、报告、记录法规的约束，除非遇到一些例外情况。虚拟货币用户不涉及货币服务业务，因此无须接受FinCEN的监管。

中国人民银行南京分行的洪蜀宁应该算是我国体制内最早公开研究比特币的人，早在2011年10月，他就在《中国信用卡》杂志上发表了题为《比特币：一种新型货币对金融体系的挑战》的文章，并对政府提出了3点建议：

1.政府和中央银行应正视比特币的存在，主动出击，动用国家巨大的计算能力，抑制私人挖掘的动力，将绝大多数比特币集中在国家手中。

2.研究成立比特币银行，在比特币交易中推行中间机构，以消除其匿名性，使其可以被监管。

3.国际联合发行比特币本位的信用货币，从而促进非主权货币体系的建立。通过这种新型的国际结算货币来挑战美元的霸权地位，使国际金融体系更加和谐、稳定。

主流资金进场

一般来说，资金都是逐利的，而其中又以风险投资资金的反应最快、最灵活。创业投资产业链的完善、对新事物的开放态度使得美国的风投基金可以迅速进入比特币相关的创业公司。而由于硬件制造业发达，中国在矿机制造领域也几乎占据了垄断地位。虽然目前国内没有相关条文对比特币领域的

投资进行规范和保障，但还是阻挡不了资金迅速进入的趋势。

早期风险投资

美国已经有大量相关的创业公司，而且其中有相当数量的企业已经获得机构投资，其中不乏知名投资机构，包括美国著名创投公司Y Combinator、美国著名风投机构USV、美国国际数据集团等。

除了老牌的风投机构外，一些新机构或基金也在其中显现身影。

据媒体报道，2013 年 5 月，美国 60 多位投资者组建了比特币创业投资机构BitAngels，募集 600 万美元，将为比特币创业公司提供资金和孵化器。

于 2012 年在纽约市成立的自由城市风投宣布，其总额 1500 万美元的数字货币基金将全部投资于比特币及其他数字货币创业公司。

在大众还在探讨比特币是否是骗局的时候，这些顶尖的跨国投资机构已经悄然在比特币领域渗透和布局。

光速创投公司董事总经理杰雷米 · 刘在TechCrunch上发文阐述了他对比特币的看法，并分析了投资机会，他认为创业公司可以在虚拟钱包、汇兑和支付 3 个领域大展拳脚：

1.虚拟钱包。虚拟钱包服务帮助用户持有比特币，提供银行活期存款账户的一些功能。如Coinbase等。

2.汇兑。汇兑服务将美元兑换为比特币，或将比特币兑换为美元。如Mt.Gox等。

3. 支付。支付服务帮助商户在交易中接受比特币支付。如专为比特币提供支付解决方案的Bitpay公司等。

全球首只比特币基金留悬念

2013年7月初，美国的文克莱沃斯兄弟向美国证券交易监督委员会提交了文克莱沃斯比特币信托基金的证券上市注册登记文件，计划最高募集金额约为2 000万美元，旨在令投资者通过划算的、方便的方式进行比特币投资，并最小化其信贷风险。该基金若能够成功上市，将是第一个追踪比特币之类的数字资产价值的交易型开放式指数基金。

目前来看，该基金能否顺利发行还是个未知数，因为除了FinCEN外，包括美国商品期货交易委员会、国税局和美国证券交易监督委员会在内的主要监管机构都未对比特币以及其他数字资产的监管提供过任何指导，或者发表过任何官方意见。但从长远来看，随着比特币拥护者的逐渐增加，比特币相关的金融产品被主流金融机构接受只是时间问题。

国内资金风起云涌

中国由于拥有丰富的硬件产业链经验，在比特币矿机的研发和生产上具有天然优势。凭借技术和资金，中国轻松地占据了先发优势。目前，全球知名的矿机生产商有南瓜张阿瓦隆、烤猫、蝴蝶矿机（Butterfly）、KncMiner、Bitfury、100TH、神鱼、彩贝、42btc、QQagent、Garden等。其中，部分自

主生产芯片，也有一部分采用其他公司现成的芯片。

在矿机的生产过程中，常常用到众筹和预付款，这是件很有意思的事情。

当初烤猫要做集成矿机，众筹发行了40万股份，以每股0.1比特币的价格筹集了4万比特币后动工。矿机做成后，该公司通过自己挖矿和销售矿机获得收益。烤猫的算力一度占据全网运算能力的20%左右，股票价格最高达到5比特币，每周三的分红以及股票的增长让早期投资者获得了巨大收益。目前，由于其算力占比降低，股票价格缩水为每股2.5比特币左右，总市值为1亿多美元。

南瓜张的第一批阿瓦隆矿机也是采用预付款形式，敢于大胆尝试的前两批预订者就像拿到了印钞机一样，每天制造大量财富，其收益超过10倍。由于芯片是矿机最核心的技术，南瓜张的经营策略后来发生了变化，开始单独销售溢价能力高的芯片。

紧接着，比特币知名人士、“90后”在校生“七彩神仙鱼”发起了Bitfish V1 ASIC矿机生产项目。他只是通过QQ（腾讯公司出品的即时通信软件）群发了几个消息，短短一个晚上就筹集了3 000比特币，并订购出去了3万个芯片。拿到样片的他于2013年6月29日在上海的深度比特币沙龙现场演示了第一台研制成功的4模组Beehive（蜂巢式）矿机样机。

由于早期挖矿收益预期高，而拿到芯片后制造矿机的门槛并不高，短时间内出现了大量的矿机芯片代购生产托管公司，但因为南瓜张的芯片最后并没有能够及时发货，所以原本预期的较高的投资收益无法保证。除了

神仙鱼的项目等少数几个项目，大部分项目均出现了大面积的投资人亏损，引发了很多纠纷与不满。

虽然至今国内官方没有对比特币进行界定与监管，但资本早已介入并在其中布局。当然，这种资本投入都存在一定的法律和收益风险。很可能正是出于法律方面的考虑，国内传统的风投基金相对谨慎和低调。

比特币金融衍生品内容丰富

比特币共计10多亿美元市值，在全球金融市场中所占的比重非常小，还处于早期发展阶段，这与其目前所引起的争议和获得的关注极不相称。但如果你留意观察比特币的产业链就能够发现，各种金融工具已经在里面得到了很好的运用。

众筹、基金、债券、股票、期货都已经取得了一定的发展。在这个领域，名声和信任至关重要。比特币圈子里的名人发起什么项目，很多人都愿意选择信任和尝试。同样，如果你一旦名声变坏，在这个行业内就很难再被认可了。

以比特币为媒介的投资环境已逐步形成。有人发起众筹做矿机，有人发起基金投资产业链，有人发行债券，有人搭建期货市场，有人筹备银行。参与这些投资的一般都是长线看好比特币的人，他们都在想办法获得更多的比特币。他们相信比特币比纸币更加接近货币的本质。不论是基金还是股票，一旦被认定是稳定获得比特币的投资渠道，其获得的认可和追捧相当惊人。

无处不在的风险

比特币本身的特性导致了种种风险，因此那些盲目贪图发财机会而进入的新人很容易遭受损失。要知道，不论传统行业还是新兴的互联网行业，所有投资都是以了解和熟悉为前提的，人云亦云的跟风操作只能使自己沦为被宰割的对象。在自媒体时代，独立思考能力至关重要。

价格的涨跌无度

从创新的传播来看，比特币还处在中早期，距离成熟状态尚远。在有百万人群参与的情况下，其市值仅有十几亿美元，市值过小使得价格容易被庄家操控，因此暴涨暴跌的现象在短期内很难被制止。比特币的价格能在两个月内上涨 10 倍，也能在一个星期之内跌掉 80%，这对于很多短线投资比特币的人来说是最大的风险。

比特币本身的技术风险

比特币本身的技术风险是永远悬在用户头上的达摩克利斯之剑。区块链分叉事件虽然在一天之内就得到了妥善解决，但的确让很多人意识到了比特币隐藏的巨大风险。在分叉的时候，如果出现拥有巨大算力的对手，完全有可能将比特币带入万劫不复的死亡之地。

对于技术问题，普通的比特币参与者相对难以理解，而且无能为力。这

种信息不对称同样构成风险。但反过来想，比特币客户端是开源的，所有原始数据都可以从比特币网络获得，比特币社区对各种技术问题的公开讨论可起到足够的风险警示作用。分叉事件的及时解决也显示出社区号召与算力投票的强大纠错功能，彰显了比特币的自我修复能力。与传统的中央银行系统相比，比特币网络更加透明，其技术风险并不比后者高。

也就是说，虽然从理论上讲比特币的技术风险较大，但是作为一个不断演进的系统，这种风险基本上可控，技术问题也不是比特币面临的最主要的问题。

交易平台的风险

除了场外的大单交易，交易平台是绝大部分比特币爱好者买卖比特币的地方。由于离钱比较近，且账户资金额度较大，交易平台是整个比特币系统中最容易受到黑客攻击的环节。

常见的黑客攻击都配合做空操作以获得利益。在比特币价格虚高时，黑客们借币做空，然后组织大规模分布式拒绝服务攻击使交易平台瘫痪，引起恐慌，造成大规模抛盘，他们再在底部接单买入。

这种手段在买卖频繁、交易量较大的时候很容易达到目的，但如果频频采用，制造的恐慌效果就一般了。

另外还有一种方式，即直接以盗取比特币账户资金为目的的入侵，国内某交易平台就曾因遭受这类攻击而丢失数量可观的比特币。

除了这些外在的攻击，交易所自身参与比特币的买卖也是很多人担心的问题。如果一个平台的大量用户在币值大跌时无法卖出，或在高涨时无法买入，却有个别人在那段时间内达成了交易，基本可以判定这样的平台自己也买卖比特币。除了对用户不公平，交易所的“自营业务”一旦仓位控制不好，造成大规模亏损，风险很可能会转嫁到用户头上：损失严重的交易所可能会卷钱逃窜，用户血本无归；损失较轻的交易所可能会导致用户无法提现。

由于比特币法律地位不明确，即使用户因权益受到侵害而发起诉讼，也很难被法院受理，追回损失的可能性较小。因此，在进行比特币交易时，选择一家诚信、可靠、稳定的交易所至关重要。

山寨币的暴富诱惑

现在比特币的价格高、开采难度大，市值缺乏进一步暴涨的空间。而很多拥有技术实力的开发者就模仿比特币的原理，号称做一些改进或者优化，推出自己的虚拟货币。这类虚拟货币通常被称为山寨币，山寨币是否有价值也是人们一直争论的焦点。

一些人认为，山寨币毫无价值，通过简单的逻辑思考就能想明白；另外一些人认为，既然比特币的本质是一套支付系统，山寨币相当于比特币之外的另外一套支付系统，而只要有人使用，支付系统就有其存在的价值。在矿机大量发货的当下，显卡矿工的阵地转移显然对山寨币是一个利好消息。

山寨币同比特币一样，普遍信任是价格的基础，只要有人相信，就会有

价格。除了已经具有一定规模因而相对较安全的少数山寨币外，不安全的山寨币是很多人的噩梦。中国币（CNC）一类的山寨币因为登上了交易平台BTC-e，其价格曾经一度很高，后来因为各种原因不被人接受，价格也随之一路暴跌，成为烫手山芋。

比特币常被人诟病的一个地方是，巨大的验证运算能力被浪费掉了。于是，有人设想利用这些巨大的运算能力做点儿事，比如解决数学难题，素数币（Primecoin）由此诞生。它号称是首个挖矿运算有实际价值的加密货币，要放弃“无用”的哈希算法，以找素数长链的方式进行工作量证明。除此之外，它还在难度调整、时间确认、总量自我调整等方面做了一些改动。

在刚刚诞生的短短半个月内，伴随着质疑和追捧，素数币价格在一个星期内从0.002比特币一路飙升至0.017比特币；在热度过去后，价格又逐渐跌回0.004比特币左右。所以，投资山寨币请务必谨慎。

期货矿机的期货风险

最早拿到集成矿机的矿工都获得了较大收益，投资回报动辄数十倍。这些财富神话极大地刺激了比特币新手。他们疯狂地涌入挖矿这个表面上可以用低成本获得大量比特币的领域。这也是南瓜张接受芯片预订后，会有这么多人参与的原因，殊不知这些投资中的很大部分可能是难以收回成本的。

比特币挖矿投入实质上是一个博弈的过程：如果大家都不投入新装备，只有你的运算能力增加了，你的盈利就会增加；如果大家都投入新装备，全

网运算能力暴涨，每个人的盈利可能维持不变，但如果你不增加算力投入，盈利就会下降。这一点在期货矿机上则表现为：你按照当前的算力估算矿机到手后的收益，似乎前景很光明，但几个月后拿到矿机时，你的收益只有当前的几分之一，可能根本就无法收回成本。

举例来说，假设每个月比特币的整网算力提升 25%，或者说每个矿机的收入减少到上个月的 80%，而你以 10 比特币的价格预订了一台 5 个月后才能到手的矿机，按照当前的情况估算，每月该矿机可以挖 4 个比特币，5 个月挖 20 个，足以收回矿机成本甚至还有一倍的收益。但事实上，你的矿机 5 个月后才到货，到货的当月你只能挖到 1.31 个比特币，而下一个月只能挖到 1.05 个。一直挖下去，最终你累计挖到的比特币也就 6.55 个，这意味着你永远都收不回成本。

不要以为这个数据很夸张，真实的算力增长其实更夸张。2013 年 6 月 1 日的算力是 90TH/s左右，而 3 个月后的 2013 年 9 月 2 日的算力高达 700TH/s左右，增加了大约 6.7 倍。照此计算，每月矿机的收入仅为上个月的 50%左右。因此，投资矿机一定要合理估算整网算力的变化，进而计算收益。投资期货矿机更需要估计等待期间的算力变化，其风险更大。

从以上的分析可以看出，比特币领域的风险无处不在。所以，想明白以下几点很重要：你赚钱的逻辑是什么？凭什么你能赚钱？你赚的钱从哪里来？只有严密的逻辑才是最可靠的。既然你已经相信了比特币这样的纯数学逻辑的产物有未来，那么请在投资的时候，多思考下你赚钱的逻辑。

03 比特币技术解密

金属货币的世界靠天然的产量限制货币发行量，靠天然的化学属性进行防伪，靠天然的珍稀性保证购买力。

纸币的世界靠中央银行的领导和经济专家决定发行多少货币，靠不断提高制作工艺和更高级的验钞机进行货币防伪，靠国家力量来保证购买力。

而在比特币的世界，上面的规则通通失效。数字世界有自己的规则：通过数学，更确切地说是通过密码学保证比特币种种天方夜谭般不可思议的特性。

比特币数学基础

密码学和协议

说起密码学，大多数人想到的可能是摩斯电码、移位加密、字符替换之

类的东西。在各种侦探小说里，“字母e在英文里的出现频率最高”这种基本的破解方法也被很多人熟知。但真正说到密码学的研究内容，大家其实都比较陌生。密码学关注的事情主要有两点：一是加密解密的数学算法本身，二是如何在现有算法基础上实现各种安全需求。

这两点有什么差别呢？以防止“消息泄露”举例，我们首先想到的是防止消息在传输过程中被第三方截获，比如说话被偷听、邮件被偷看、网络数据被窃取。而事实上，小偷是防不住的，但我们可以保证数据即使被偷了，窃取者也无法使用。只要双方事先约定一套加密解密的方法，以密文的方式传输信息，就可以有效地防止信息泄露。

但有时候消息泄露的内涵比这更复杂，加密算法的方案并不适用。设想一下，公司某小组有10个员工，他们都想知道组内平均月薪是多少，但都不愿意透露自己的月薪数额，公司制度也不允许讨论薪水。有什么办法可以既得到答案又不泄露各自薪水数额呢？其实办法很简单，甚至不需要用到密码学知识。第一个人随便想一个大数，比如12 345，接着在纸上写下自己月薪与这个数字之和并传给第二个人；第二个人再在这个数字上加上自己的月薪，然后将最新数字写到另一张纸上传给第三个人；直到最后一个人把纸条传回第一个人，第一个人用字条上的最终结果减去只有自己知道的12 345，就得到了所有人的月薪总和，而且每个人都没有泄露自己的薪水。

以上两类情况分别对应了密码学的两个研究方向：密码学不仅研究加密解密的数学算法，更多时候，它还研究保护信息安全的策略，我们称之为“协议”。

哈希算法

现在设想这样一个场景：爱丽丝和同学鲍伯商量明天早上谁先去教室打扫卫生。两个人都不想去，于是鲍伯想了一个办法："我扔一枚硬币，你猜一下是正面朝上还是反面朝上。如果猜对了，我去打扫卫生。如果猜错了，嘿嘿……"如果爱丽丝和鲍伯此时是面对面地站在一起，那么这个策略当然没有问题，可以说相当公平，甚至可以用更简单的办法，比如石头剪子布。可是，如果他们是通过网络聊天的方式商量，那爱丽丝显然不会同意这个办法，因为她担心自己无论猜正面还是反面，鲍伯都会说她错了。

有什么办法可以保证通过网络聊天的方式也能做到公平扔硬币呢？有人会说，那我们给扔硬币的结果加个密吧。现在假设任意奇数都代表硬币的正面，任意偶数都代表硬币的反面。鲍伯随便想一个数，然后乘以另外一个数，把结果先告诉爱丽丝，比如 1 234 × 531 = 622 254，鲍伯想的是 1 234，然后把 622 254 这一结果告诉爱丽丝，并声称另一个秘密数字 531 是密钥，由他自己保管。但这样做显然也不行，因为验证结果的时候，鲍伯可以谎称 1 234 才是密钥，531 是原始数字，这样鲍伯依然立于不败之地。但是如果鲍伯事先把密钥公布出来呢？这样也不行，因为爱丽丝知道密钥后就能直接计算出原始数字，便失去了保密作用。

传统加密方法不能公开的原因是知道了加密方法也就知道了解密方法，只需要反向计算就能解密。那么，有没有一种加密方法，使得即使知道了加密方法，也不能恢复出原文呢？有的，我们只需要在加密过程中加入一些不

可逆运算就行了。这次鲍伯又设计了一种新加密方式：

1.鲍伯先设想一个数，并加上 123 456。

2.把结果平方，取第 3~10 位，组成一个 8 位数。

3.再用这个数除以 456 789 求余数，然后把这个结果告诉爱丽丝。

4.爱丽丝猜测鲍伯设想的是奇数还是偶数。

5.鲍伯告诉爱丽丝原始数字，爱丽丝按照上面的过程再计算一遍，看结果是否和鲍伯给的结果一致。

假设鲍伯想的依然是 1 234，按照上面的过程依次得到：

1 234+123 456 = 124 690

124 690 × 124 690 = 15 547 596 100

54 759 610 mod456 789=401 719

（Mod 表示除法求余数）

爱丽丝拿到的结果是 401 719，既可以验证鲍伯有没有撒谎，同时爱丽丝又很难根据 401 719 反向算出 123 456。

这样也不能绝对保证鲍伯不作弊，但如果鲍伯想作弊，他就必须事先找到一奇一偶两个数，它们按照上面的运算能得到一样的结果。这个难度取决于上面算法的难度。

在密码学中，这种会丢掉一部分信息的加密方式被称为“单向加密”，

也叫作哈希算法。

一个可靠的哈希算法至少需要满足下面几个条件：

1. 对于给定的数据M，很容易算出哈希值X = F（M）；

2. 根据X很难算出M；

3. 很难找到M和N令F（M）=F（N）。

真实世界的哈希算法比上面的过程要复杂得多，但原理是类似的。而且即使对于很长一段数据，仅仅改变一个字母，也会造成二次哈希结果的巨大差异。被认为安全且在互联网中被广泛使用的哈希算法包括MD5（消息摘要算法第五版）、SHA-256 等。比如“1 234”使用MD5 算法计算的结果是“81DC9BDB52D04DC20036DBD8313ED055”，而用SHA-256 算法计算出的结果是“03AC674216F3E15C761EE1A5E255F067953623C8B388B4459E13F97 → ← 8D7C846F4”。哈希算法的结果长度都是固定的，从上面看，MD5 的结果长度为 32 个字符，SHA-256 则达到 64 个字符，所以SHA-256 看起来更安全一些，更难找到能算出相同结果的M和N。

这种单向加密算法并不能用来进行普通的信息传输，更多是用来进行传输结果的准确性验证。很多下载网站都提供了下载文件的原始MD5 值供校验，以防止文件被病毒修改。常用的BT（比特流）下载也是通过特定的哈希算法来确认每一部分数据是否下载完成。

非对称加密

现在我们来看一下在真正要进行信息传输的情况下应该怎么办。

同样假设爱丽丝和鲍伯要通过互联网传输一份绝密情报，那么，如何阻止第三方在网络上截获信息呢？如果是一般情况，可能的步骤是使用文件压缩工具，比如WinRAR对文件进行加密压缩，然后通过电子邮件或者QQ把加密的文件发过去，为了更安全，或许还会发短信或者打电话把解压密码告诉对方。但是作为绝密情报传输的操作人，面对的可能是国家机器，所有的网络和通信工具都处于被监听状态，如果按照上面的过程，依然会造成信息泄露。如果想办法把密码加密后再发过去，但是给密码加密的方式又该如何确定呢？如果爱丽丝和鲍伯事先认识，或许可以见面并约定将出生日期加上手机号作为密码，但更多情形下，双方并没有可以利用的公共秘密。

传统密码世界一直需要面对这样一个看似死循环的无解问题。这里我们有两种思路可以尝试解决。

第一种，专门设计一个秘密的加密算法，使对方即使拿到密码也没有办法解密。如果是绝对的军事需求、能邀请高水平的数学家来确认算法的安全性，这样确实没有问题。但如果是互联网通用技术，如果不公开算法的细节，恐怕没有人肯使用。密码学世界有一个柯克霍夫原则：即使密码系统的任何细节已为人熟知，只要密钥（key）未泄露，它也应是安全的。无论是在战争时期还是和平时期，都不能把保密的希望寄托于系统或算法的秘密性。机械可以拆解，软件可以反编译。密码系统的所有细节总会被有心人一一拆解。这个时

候，如果系统符合柯克霍夫原则，那么即使对手拆解了系统但不知道密钥，他也没有办法破译加密的信息。满足这种严苛条件的密码系统才是安全的。

第二种方法更绝。要是有一种加密系统，加密和解密使用不同的密码，假设有2个密码A和B，使用A对数据M进行加密得到加密数据X = F(A,M)。但是，知道A和X无法解密出M，必须用另一个密码B使得数据还原M = F（B,X)。爱丽丝只需公布密码A，鲍伯使用公开渠道拿到的A对情报进行加密，再通过任意方式发给爱丽丝进行解密，这样一来，即使所有的通信被监听，对手也不可能拿到情报。当然，这里依然有一个缺陷，即鲍伯如何确定自己拿到的密码A确实是爱丽丝给出的，而没有被别人替换掉，不过这是另一个关于可信认证的话题，暂时不在这里讨论。

如果使用我们设想的这些神奇加密算法，似乎问题就可以迎刃而解了，但问题是，这样的技术存在吗？听上去似乎并不可能，因为从直觉上判断，知道了加密方法就一定知道解密方法，只需要反过来计算就可以了。加密方法和解密方法是否可能不对称？

有可能！我们来看一个小时候经常在《趣味数学》这类书里看到的数学小魔术：让对方任意想一个三位数，并把这个数和91相乘，然后说出乘积的最后三位数，就可以猜出对方想的是什么数字。比如对方想的是123，那么对方就计算出123×91 = 11 193，并把结果的末三位193告诉我。看起来，这么做似乎损失了不少信息，我可能没法反推出原来的数。不过，我仍然有办法：只需要把对方告诉我的结果乘以11，乘积的末三位就是对方刚开

始想的数字了。可以验证一下，193×11=2 123，末三位正是对方所想的秘密数字！其实道理很简单，91 乘以 11 等于 1 001，而任何一个三位数乘以 1 001 后，末三位显然都不变（例如 123 乘以 1 001 就等于 123 123）。先让对方用他所想的数字乘以 91，假设乘积为X；我再在X的基础上乘以 11，其结果相当于我俩合作把原数乘以了 1 001，末三位自然就变了回去。X乘以 11 后的末三位是什么只与X的末三位有关，因此，对方只需要告诉我X的末三位就行了，这并不会丢失信息。知道原理后，我们可以构造一个定义域和值域更大的加密解密系统。比如，任意一个数字乘以 400 000 001 后，末八位都不变，而 400 000 001=19 801×20 201，于是你乘以 19 801，我乘以 20 201，一个加密解密不对称的系统就构造好了。我们甚至还可以构造一个更大的系统：4 000 000 000 000 000 000 000 000 000 001=1 199 481 995 446 957×3 334 772 856 269 093，这样我们就成功构造了一个 30 位的加密系统。这是一件非常酷的事情，任何人都可以按照这个方法加密一个数字，但是只有自己才知道怎么把所得的密文变回去。

但如果仅仅按照上面的思路，如果对方知道原理，知道我要构造出带很多 0 的数，根据 19 801 和 8 位算法这两个条件其实可以比较容易地穷举出 400 000 001 这个目标值。要解决这个问题，我们来看看真实世界是怎么处理的。

RSA 算法与椭圆曲线算法

直到 1976 年以前，所有的加密方法都是同一种模式：

1. 甲方选择某一种加密规则，对信息进行加密；

2. 乙方使用同一种规则，对信息进行解密。

由于加密和解密使用同一种规则（简称“密钥”），这被称为“对称加密算法”。这种加密模式有一个最大的弱点：甲方必须把加密规则告诉乙方，否则无法解密。这样一来，保存和传递密钥就成了最让人头疼的问题。尤其是人数多了之后，每两个人都要互相商量一个密钥，复杂性大大提高，而传递密钥则带来更高的安全风险。

直到1977年，李维斯特、沙米尔和艾德曼设计了一种算法，可以实现非对称加密。这种算法用他们三个人的名字命名，叫作RSA算法。直到现在，RSA算法一直是应用最广泛的非对称加密算法。毫不夸张地说，只要有计算机网络的地方，就有RSA算法。这种算法为什么这么晚才出现？或许类似的技术一直隐藏在“二战”的迷雾中不为人知。

这一非对称加密模式的流程如下：

1. 乙方生成两把密钥（公钥和私钥）。公钥是公开的，任何人都可以获得，私钥则是保密的。

2. 甲方获取乙方的公钥，然后用它对信息进行加密。

3. 乙方得到加密的信息后，用私钥解密。

由于公钥加密的信息只有私钥解得开，因此只要私钥不泄露，通信过程

就是安全的。

RSA 算法为什么更加安全呢？在数学世界里，有一些公认的、需要消耗极大计算量才能得出结果的难题，比如大数因式分解问题、离散对数问题、椭圆曲线问题。RSA 算法正是用到了大数分解这一相当犀利的不对称难题。比如对于我们上面构造过的 30 位加密系统：4 000 000 000 000 000 000 000 000 000 001=1 199 481 995 446 957×3 334 772 856 269 093，反过来算乘积非常容易，但是要把 4 000 000 000 000 000 000 000 000 000 001 分解成后面两个乘数，在没有计算机的时代几乎不可能成功！而一旦数字长达数百位，即使是超级计算机也需要耗费海量的时间来计算才有可能，下面给出两个近年来的大数分解记录。

大数因式分解记录RSA200，一个共有 200 位的非特殊数字，在 2005 年，计算机花了 18 个月时间才把它分解成两个素数。2007 年 3 月 6 日，一个国际组织打破了这个保持了两年之久的纪录，来自 3 个机构（洛桑联邦理工学院、波恩大学、日本电话电报公司）的计算机集群在经历了 11 个月的计算后，终于成功地把一个有名的很难分解的大数——2^1039-1 分解为素数因子。消息爆出后，一个匿名人士在网上贴出了下面的等式：

2^1039-1=p7×p80×p227

p7=5 080 711

p80=558 536 666 199 362 912 607 492 046 583 159 449 686 465 270 184 →

← 886 376 480 100\52 346 319 853 288 374 753

p227=207 581 819 464 423 827 645 704 813 703 594 695 162 939 708 007 →

← 395 209 881 208\387 037 927 290 903 246 793 823 431 438 841 448 →

← 348 825 340 533 447 691 122 230\281 583 276 965 253 760 914 101 →

← 891 052 419 938 993 341 097 116 243 589 620 659\72 167 481 161 749 →

← 004 803 659 735 573 409 253 205 425 523 689

其中p7是已知的，p80×p227则大概是人类已经分解的最大整数（307个十进制位）。

椭圆曲线算法（ECC）则是另一种著名的非对称算法，在比特币体系里占据重要地位，是比特币钱包安全性的密码学基石，也是比特币被称为密码学货币（Cryptography）的原因。

ECC各方面的性能和RSA比起来几乎完胜：

1. 安全性能更高。比如160位ECC与1 024位RSA有相等的安全强度。

2. 计算量小，处理速度比RSA快得多。

3. 存储空间占用小。密钥尺寸和系统参数与RSA相比要小得多。

4. 带宽要求低。

ECC的这些特点使它逐渐取代RSA，成为通用的公钥加密算法。

比特币初接触：客户端的使用方式

客户端下载

首次使用比特币需要先下载客户端，可以在http://bitcoin.org上选择不同种

类的钱包软件。目前，钱包软件包括电脑钱包、手机钱包和在线钱包。从易用性和传承性的角度考虑，这一部分将以最早出现的客户端Bitcoin-QT为例。

下载、安装后，Bitcoin-QT首次运行时需要花费一段较长时间进行数据同步，目前同步的数据量在10G左右。之所以有这么大的数据量，是因为Bitcoin-QT会下载比特币有史以来的所有交易记录（有些轻量级客户端可直接从网络实时查询结果，无须同步如此庞大的文件）。待数据同步完毕，“余额”和“未确认”项显示的数据就是最新数据。

比特币地址

将Bitcoin-Qt切换到“接收”菜单，可以看到软件已经自动生成了一个地址，那一长串乱码般的字符就是我们的收款账号。至于这一长串东西是什么意义，凭什么作为账号，后文会统一回答。

比特币支付

为了支付，我们需要创建一个目标地址。可以在“接收”菜单下通过“新建地址”功能直接创建一个标签为“test”的新地址。然后，在“发送”菜单下填上新创建的地址和要发送的金额，点击“发送”，这笔“钱”就发出去了。待网络确认完成，将发送到我们的新账户“test”上。在“交易记录”菜单下就可以看到我们的操作记录以及网络确认次数，当确认次数达到6次，此次交易便宣告成功。

如果需要用手机钱包支付，手工输入这么一长串地址显然是令人担心的（其实输入错误肯定无法发送成功，因为错误的地址无法通过特定的算法验证）为解决这一问题，Bitcoin-QT提供了二维码的操作方式，直接用“接收”菜单的“显示二维码”功能就可以另存为图片并把二维码发给对方，让对方通过手机扫描的方式直接支付，甚至可以直接填上希望支付的金额并生成带额度和消息的二维码。

因为每个比特币地址上的金额流水全部是公开的，如果希望保密或者区分不同的付款人，可以为每个人单独生成一个地址并提供给对方，而不是像现实银行账户那样，要求对方增加一个尾数用于确认。在这里，每个人都可以为自己创建任意数量的账户（地址）。

备份钱包

比特币的钱包数据是保存在本地电脑上的，万一出现系统崩溃或者中毒事件，导致数据丢失该怎么办？Bitcoin-QT提供了钱包文件备份功能，点击“文件”菜单下的“备份钱包”就可以把钱包文件导出，保存到安全的地方。而恢复钱包也比较方便，只需把备份文件拷贝回上面的目录，重新打开Bitcoin-QT就可以看到备份钱包中的金额了。

加密钱包

在通常情况下，如果你的钱包文件被别人拿到，那么对方将拥有你所有

额度的绝对支配权。这太危险了，尤其是当电脑中毒时。

Bitcoin-QT同样考虑到了这个问题，其应对之策就是支持给钱包加密。在“设置”菜单下的“加密钱包”选项里可以设置密码，钱包加密功能会保护所有在该钱包中生成的比特币账号。这个密码类似支付宝的支付密码，付款时需要输入，这样即使对方偷走了钱包文件也只能看余额而不能转账。

比特币再深入

上面简单介绍了比特币的使用，接下来，我们会思考一些更深入的原理问题，比如在一个没有中心的系统中如何产生有中心的效果，并将看到前面大段的密码学知识是如何建立起整个比特币系统的。

去中心化思想

百度百科“比特币”词条是这样定义比特币的：比特币是一种由开源的P2P（Peer-To-Peer，点对点）软件产生的电子货币，是一种网络虚拟货币。比特币不依靠特定货币机构发行，它通过特定算法的大量计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。

这段描述充斥着计算机技术界的行话，但其最核心的思想很清晰——去中心化。去中心化的意思就是不由某个人或某个群体主导一切，而是大家集

体参与、共同决定。在沟通方式低效的年代，这是一件非常奢侈的事情，但由于能够保障所有人的权利、及时纠正可能的错误，所以人类社会形态也遵从这个思想，从中心化不断迈向去中心化。

进入互联网时代，由于沟通的便利性得到极大提升，去中心化思想开始在各领域迅速扩张，任何人都可以在网络上表达自己的观点或创造内容。比如在读这本书时，你可能就一边翻着百度百科的词条，一边在豆瓣书评里吐槽，同时还可能在微博里搜索别人是怎么评价比特币的。总而言之，在去中心化的世界里，所有人都是平等的，你可以给 9 分的电影打 2 分，但无法因此把 9 分拉低到哪怕 8.9 分；你可以宣传自己，但无法封杀别人的观点。

“比特币之父”中本聪在设计比特币模型时就将其设定成去中心化，其P2P网络模型和Facebook的架构类似。事实上，当技术条件成熟时，把去中心化的思想引入任何领域都将引爆群体智慧，都意味着这个领域将发生颠覆性的变革，正如博客之于出版、微博之于媒体、Facebook之于社交、网游之于娱乐、选票之于政治。就连极度中心化的苹果也是因其去中心化的开发平台App Store（应用商店）而大获成功。比特币则悄悄打开了金融业去中心化的第一扇窗户，这是第一个没有中央银行的货币体系，其货币的发行总量、发行速度、支付验证方式在一开始就由去中心化的数学模型设定。

P2P架构和安全通信

上网时，我们经常遇到的是C/S架构（客户机/服务器架构），例如新浪

微博。这种架构的原理就是，大家一起连接到weibo.com，所有信息都储存在新浪服务器上，我们通过服务器中转信息进行交流。这种架构的优点是简单快捷，但容易受到攻击。假如黑客把新浪微博黑了，或者新浪微博关了，整个体系就崩溃了。

还有一种架构叫P2P架构，例如下载工具电驴就属于这一种。这种架构的特点是：服务器并不是必要条件，每台联网电脑都是一个独立的个体，通过网络联到其他几台甚至成百上千台电脑，最后全球的电脑形成一个密密麻麻的网络。P2P网络的一大特点就是，一旦启动，就无法关闭。

在这个P2P网络上的所有电脑都直接或者间接地联通起来，某个节点上发出的信息最终可以扩散到全球所有的节点。举例而言，A在中国，B在美国，A和B的联通方式可以是直接连接，也可以是通过位于欧洲的C的电脑搭桥间接地连接。

P2P网络的联通不成问题，但是信任的问题比较突出。例如，A发出一条信息，目标对象是B，B通过P2P网络最终接收到此信息——可以是直接从A电脑传递过来的，也可能是通过多台电脑转手传递过来的——B会产生两个问题：第一，这条信息到底是不是A电脑发送的？第二，信息传递过程中如何确保不被帮忙传递信息的C、D甚至更多人偷窥到信息原始内容。

这就回到了我们讲过的非对称加密技术。在刚才的例子中，假如A要发送一条信息给B，确保这个信息只有B才能解密，那么A就用B的公钥（公钥是公开的，整个P2P网络都知道B的公钥）加密原始信息，这条信息传播

到整个P2P网络，虽然所有电脑都有B的公钥，但是用公钥无法解密这条信息，最后B收到这条信息，用自己的私钥就能够轻松地解密这一信息。

那么，A怎么证明自己是这条信息的发送者呢？在网络上，任何人都可以把自己伪装成任何人，B收到信息时，可能传递信息给B的那台电脑会声称它就是A，那么B是否就轻易相信那台电脑就是A呢？不能，因为很可能是那台电脑伪装成A。

A要想证明给B的信息是由自己发出的，只需完成下面这两个步骤：第一步，用A的私钥对原始信息做第一层加密；第二步，在上一步获得的数据基础上再用B的公钥做第二层加密。第一层加密的目的是为了证明这个信息是由A加密并发出的，因为只有A的私钥才能完成这样的加密，这一步也叫作数字签名；第二层加密的目的是确保信息只有B能够解密，因为B的私钥只有B电脑才有。

B收到这个加密的信息后，以相反的顺序做两次解密操作即可：第一步，用B的私钥解密收到的信息；第二步，在第一步获得的数据基础上用A的公钥再次解密。第一步顺利完成，可以确保信息只有B自己能够解密，其他人是无法解密的；第二步顺利完成，B就获得了原始信息，同时也表明这条信息确实是由A的私钥加密生成，排除了是被别人伪造的可能。

有了这一技术保障，即使在匿名的互联网环境中，我们也不必再纠结于通信的安全性，而可以将注意力集中在比特币的体系架构上来。

比特币的本质

在网络上浏览比特币相关的网页时，总是可以看到各种印着“B”符号的硬币，仿佛那就是比特币。实际上，那只是爱好者自己铸造的玩具，和比特币没有丝毫关系。比特币并不是任何有形的硬币，也不是大家想象的一段数据，同样也没有办法把某些比特币从整个系统中分离出来。比特币的本质是一个互相验证的公开记账系统，其工作就是记录所有账户发生的交易。每个账号的每一笔资金流动都被记录在账本里。而且，每个人手上都有一份完整的账本，每个人都可以独立统计出比特币有史以来每个账号的每一笔流动，当然，也能算出任意账号当前的余额是多少。

这里最关键的一点在于：每人手上都有完整的账本，这个系统里没有任何人拥有唯一决定权。这意味着没有人可以决定向这个系统增加货币或者改变规则，因为个体的修改会被整个网络否决。除非有人可以修改 50%以上的人手上的账本，这就是比特币系统里所谓的 51%攻击。

比特币客户端Bitcoin-QT启动时会进行大量的数据同步，Bitcoin-QT只告诉我们说这是在进行数据同步，但我们并不知道这是什么数据以及为什么要这么做。实际上，同步的是比特币世界的所有交易记录，这部分数据保障了整个体系的去中心化和每个客户端的一切知情权。而不需要下载交易数据的轻客户端，如Electrum则是去几个提供交易数据查询功能的服务器查询特定账号的记录，由于这些数据全部是公开的且带有严密的校验，任何查询服务器都没有必要也不可能伪造数据。所以，即使轻客户端带来了部分中心化效果，实际上对全局的去中心化并没有什么影响。

比特币还有几个令人十分困惑的问题，就是我的地址里拥有的那些币究竟在哪里？备份钱包是把里面的币备份了吗？在现实中，我们知道钱是什么，因为可以直接掏出来看；我们也知道自己的钱在哪里，要么是现金，要么存在银行，要么在诸如证券交易所一类的机构。而比特币系统只是所有交易的记录，这里只关心某个账号里是否有币、有多少币，而币本身是抽象的，大家并不知道它具体是个什么东西。某个地址拥有的比特币数额存在每个人的客户端数据里，大家都知道你有币就可以了。所以当我们备份钱包时，其实只是在备份对自己比特币地址的所有权。

地址是什么

在现实生活中，如果需要一个银行账户，就需要去银行排队开户，然后拿到银行分配的一串数字账号，之后才能使用银行功能。而在比特币体系

里，我们的账户似乎并不需要谁来开设，本地客户端自动生成即可；我们不需要向任何第三方公布，对方就可以直接向我们的账户转账；账户的形式也非常奇特，比如 1H4AG73nXz5to9zWkH4GUZEH1Nuey8EVjJ。

刚接触比特币的用户印象最深的大概就是这一长串乱码般的地址，它给人的第一感觉是不明觉厉[①]，第二反应就是特别容易输入错误。幸运的是，绝大部分时候并不需要手工输入比特币地址，通常是通过复制粘贴或者二维码扫描的方式。即便万一需要手工输入，比特币地址的校验机制也会提醒你账号不正常，以免出错。

可是，这一串地址到底是什么？会不会和别人的重复？

这里先回忆一下前面讲过的非对称加密技术。简单来说就是通过一套数学办法，产生一对密钥A和B，若使用A加密一份数据，必须使用B来解密；而使用B来加密数据，则必须用A才能解开；而且根据A可以很轻松地计算出B，反过来则不行。A就叫私钥，B叫公钥。顾名思义，A是保密的，B是公开的。

所以，比特币地址其实就是一套非对称技术的公钥，这套技术就是椭圆曲线算法，而和公钥对应的私钥实际上就在钱包文件里藏着。因为公钥和私钥需要使用特殊的算法成对生成，所以比特币地址不能像普通密码一样人为设置，而且看起来也没有什么规律。按照私钥保密、公钥公开的原理，比特币地址可以告知任何人，但钱包文件则必须妥善保管，一旦丢失，钱包就不

① 不明觉厉，网络用语，意思是“虽然不明白是什么，但好像很厉害的样子”。

安全了，而且由于整套体系的去中心化和匿名性，没有任何人有权力或能力找回丢失的比特币。

至于地址有多少，会不会和别人的重合？可以这么形容：如果每粒沙子里面都有一个地球，那么地址数大概等于地球上所有沙子里面的地球的沙子数的总和。如果你幸运地生成了一个有余额的其他人的地址，那你真的是太幸运了！如果愿意，这笔比特币就归你了！

支付的背后

由于比特币不存在现金交易的概念，一切交易都依靠账户间的转移，所以比特币的支付概念类似于银行转账。先看一下银行的转账过程：我们首先需要填写对方的账号和转账金额，本地一般会先检查一下余额是否充足，如果充足就把这个转账请求发送到银行数据中心，银行确认密码、U盾、对方账号等信息正确后，就把保存在银行数据库中的本地账号减去一个金额，同时给对方账号加上一个金额，然后返回成功或失败的信息。

当存在银行这一官方机构时，上面的操作过程安全可靠，但比特币体系中并不存在任何类似于银行的这种可信机构，这里每个人都是平等的，同时每个人都不一定是可信的。事实上，比特币的转账机制也很简单。

假设A有100个比特币，他要转账给B。那么A写一条信息：从A的地址转账100个比特币到B的地址，然后用自己钱包里的私钥加密并将其传播到整个比特币网络上，网络上的人都用A的地址（公钥）解密验证这条信息

确实是由A发出，而通过历史交易数据计算出A的地址确实拥有100个比特币，于是整个网络公认此次转账操作，A钱包中存款减少100个比特币，B钱包中存款增加100个比特币。

非对称加密技术可以使这个转账过程顺利实现，一切看起来都非常完美，但是其中有4个隐藏的问题：

1.整个网络这么大，什么时候才算转账成功？

2.上面说的是转账体系，那么货币创造体系是怎样的？没有央行负责统一发行，A的100个比特币最初是从哪里来的？

3.A如果作弊怎么办？方法一：A如果没有100个比特币而发出转账信息，整个网络则不理会他，因为大家都拥有网络中所有的交易信息，一计算就会发现A根本没有那么多钱，因此转账无效。方法二：A确实有100个比特币，但他同时向网络发出两个转账信息，一个是转账100个比特币给B，另一个是转账100个比特币给C。由于网络上电脑非常多，网络传递也有随机性，所以有的电脑是先收到转账给B的信息，有的电脑是先收到转账给C的信息，那么最终这个网络以哪条信息为准？

4.所有账户余额都是基于历史记录算出来的，那么如何确保历史记录安全而完整？假如有人要攻击比特币体系，他没有办法伪造他人转账信息，但作为比特币体系中的一员，他如果恶意删除自己的部分历史转账记录会怎样？

比特币系统创造性地发明了“挖矿”的概念，一举解决了上述4个问题。

天才的挖矿

挖矿是比特币体系里让新人特别费解的事情，居然可以从网络上挖出比特币，从哪里挖？拿什么挖？挖矿的本质是什么？

比特币的本质就是一个互相验证的公开记账系统，而挖矿的本质就是争夺记账权！从工作内容来看，挖矿就是将过去一段时间内发生的、尚未经过网络公认的交易信息收集、检验、确认，最后打包加密成为一个无法被篡改的交易记录块，从而成为这个比特币网络上公认的已经完成的交易记录，永久保存。

在比特币的世界里，大约每 10 分钟就会在公开账本上记录一个数据块，这个数据块里包含了这 10 分钟内全球被验证的交易。所有的挖矿电脑都在尝试打包这个数据块并提交，但以谁提交的为最终结果则是需要争夺的。

争夺记账权有什么好处？最终成功生成那个交易记录块的人，可以获得伴随这些交易而生成的交易费用外加一笔额外的报酬。交易费用一般都是转出资金方自愿提供给挖矿者的，因此不是系统新增的货币；额外的报酬是新生成的比特币，这就是比特币系统新增货币的方式。

比特币的有限性就由额外报酬的数量控制。依据比特币系统的设置，大约每 10 分钟可以生产一个交易记录块，最初每生产一个交易记录块可以获得 50 个比特币的额外报酬，这意味着比特币网络每天增加 7 200 个比特币，但是该报酬每隔 4 年就会减半，因此最终整个系统中最多只能有 2 100 万个比特币。目前已经经历了第一次减半，当前每个记录块的收益是 25 个比特币。

截至2013年7月14日，被生产出来的比特币一共是1 140万个。

随着整个网络计算能力越来越强，截至2013年7月中旬，整个比特币网络的算力已经超过世界前500位超级计算机总和的20倍以上，而且这个算力还在飞速上涨。普通电脑的算力几乎没有任何机会抢到记账权。于是，“矿工”（参与者）们就自己构建矿池模式，和游戏组队打BOSS（难度较大、奖励较高且出现在最后的关键时刻的人物或怪物）一样，如果矿池抢到了记账权，那么就按照计算贡献来分配这次获得的收益。

那么，电脑是靠什么机制争夺记账权？在算力急速上升的情况下，它们又是如何使整个网络的交易记录块生成速度，保持在10分钟左右一个？事实上，电脑是在玩一个叫哈希的密码游戏，更具体点就是SHA-256算法。大家比的就是，在10分钟内谁能找到一个值和上一个数据块的哈希值以及10分钟内验证过的新交易记录合起来可以算出最小的哈希值。算出最小哈希值的那个人就抢到了记账权。同样，至少要小于某个值才有转发权，这个值越小，对应的就是比特币网络的难度系数越高。由于哈希值的结果相当随机，无法预知大小，所以只能不断苦算，纯粹是拼算力。如果在这10分钟内没能抢到记账权，那之前的努力就白费了，拿到新的区块后会重新进入下一轮。

之所以计算时要加上上一个数据块的哈希值，是因为这样一来，所有的数据块就被组成了一条可以从前到后不断验证的数据链条。修改中间任何一个数据块的任何交易记录，都会导致之后的所有数据块的哈希值验证失败；如果企图在修改记录后重新找一个合理值算出符合条件的哈希值并重新打

包，那也意味着之后所有的数据块都需要重新寻找那个值来重算哈希值，其计算速度还必须比整个比特币网络更快，只有这样才能让网络接受你的结果，这就意味着攻击者要拥有超过整个比特币网络正义部分的算力，换句话说，要使用超过整个网络 50%以上的算力才能保证攻击有效。当找到一个有效的哈希值时，就要迅速把生成的数据块转发出去，其他矿工收到后，认为这个数据块更优秀，就会以这个块为基础进行下一轮的计算。如果期间收到更小哈希值的数据块，首先考虑数据链长度，其次是哈希值更小，抛弃之前的结果，在新的基础上继续开展下一轮计算。

刚刚提到了一个很重要的概念——转发权。挖矿的难度是全网自动调整的，其依据是之前若干数据块生成的平均速度：如果低于 10 分钟，就把难度提高；如果高于 10 分钟，就自动把难度降低。这是一个默认规则，每个客户端都会独立判断并遵守，并不需要统一调度和安排。如果不遵守，你计算出来的数据块哈希值就达不到要求，也就无法得到其他矿工的认同。难度提升很简单，就是降低哈希值的下限。由于哈希算法的特性，这会使计算量呈指数上升。当找到一个可以算出达到标准的哈希值的数字后，就可以把算出的数据块广播出去，寻求其他矿工的认同。对于一次比特币交易来说，如果你的交易单正好在这个数据块中，就意味着获得了一次确认。当其他矿工在有你交易的数据块上继续工作并把数据链延长时，每延长一个块就意味着多得到一次确认。比特币网络的规则是，若一笔交易获得了 6 次确认，就认为这个交易已经得到了全网的认同，可以认定为有效。

有人可能会反驳说，如果我准备6台电脑，为我的虚假交易确认6次有效，不就可以在短时间内成功骗到别人吗？对不起，当挖矿难度变高，企图用普通电脑为别人确认交易几乎是不可能的。所以，在比特币诞生初期，Bitcoin-QT甚至自带了挖矿功能，随着全网算力的提高，这个功能纯粹鸡肋，就取消了。

比特币的其他特性

比特币作为纯粹的互联网产物，由于其纯数据特性，故而具有一些和现实货币迥异的、极具颠覆性的特点，为我们带来了另一个维度的思考。

匿名和公开

由于没有传统世界银行的开户行角色，比特币系统是纯匿名的。虽然我们可以根据本地完整的交易记录查询每个账号的流水信息，但无法将账号和现实的人对应起来。只要愿意，每个人都几乎可以拥有无数个地址。同样，没有任何人有权力操纵他人账号上的比特币。这是在人类历史上，第一次从技术上保障了私人财产的神圣不可侵犯、不可追踪、不可冻结。

然而，虽然比特币系统是匿名的，但若某个组织愿意公开自己的比特币账号，那么整个网络都可以随时追踪到该账号的所有流水信息。每一笔的到账时间、数额和支出都可以清晰地看到，相当于直接查询银行内部原始账单！对于非政府组织来说，这有助于大幅降低账目维护成本，而且能够保证

百分百透明。2013 年芦山地震时，壹基金就曾接受比特币捐赠，其比特币账目在网络上清晰可查。

纸钱包和脑钱包

只要拥有对应的私钥，就意味着拥有特定比特币地址上比特币的所有权。我们通常将私钥藏在钱包文件里，事实上，它经过编码也只是一个字符串，只是比地址略长一些，我们完全可以把它抄下来或者制成二维码打印到一张纸上，然后放到相对安全的保险柜里。那个字符串就承载了你全部的比特币财富！

基于比特币的一个更有意思的创造是脑钱包，其神奇之处完全超乎想象！在正常情况下，私钥和比特币地址一样难记，而在 http://brainwallet.org 上，通过一句话就可以生成一对公钥和私钥。只要能记住这句话，你就可以根据它再次生成私钥，在任何有网络连接的地方提取比特币。这意味着可以把自己所有的财富储存在大脑里，而不依赖任何外在的东西。但是，生成脑钱包一定要尽量选一句全球唯一的话，不然“撞车”的机会就会大大增加。当然，这其实并不难，比如想一句：木匠张小明和老婆赵小花的小儿子叫波波。这样一句话大概是很难被别人也想到的。不过由于加入了人工因素，被猜中的概率大大增加，所以脑钱包并不是特别推荐，除非你明白自己在干什么。

可证明和不可证明

想象一下，假如你使用的是脑钱包，这个世界上将没有任何证据可以证明你拥有这么一笔钱。除非失忆或者死亡，否则这笔钱将一直存在。

同样，非对称数字签名技术可以轻易证明你拥有某个地址上的财富。只需使用私钥加密一条信息并发布出来，大家就可以确认你对该账户的拥有权，而无须把私钥公开，这同样适用于证明一笔匿名支付确实是你操作的。Bitcoin-QT客户端自带这个功能。

丢失不可找回

由于比特币去中心化以及几乎不可破解的特性，如果丢失了钱包文件(私钥)，就意味着这个账号上的比特币彻底丢失了，神仙也无能为力。这里可没有拿身份证找回这码事。

当然，如果只是钱包文件的密码忘记了，那还可以尝试暴力破解；但若是钱包文件丢了，那就彻底没辙了。要知道，即使在真实世界里，许多特工的生命安全都是建立在椭圆曲线算法的强壮性上。

04 比特币生态圈

“天下熙熙，皆为利来；天下攘攘，皆为利往。”在《史记 · 货殖列传》中，司马迁深入阐述了经济利益对人类的强大吸引力。比特币起源于神秘创始人中本聪对于不需第三方监管的电子支付技术的革命性实验，经由开源社区、矿工、交易所、使用者等多方参与者的共同努力，最终形成了一个涉及数十万人、规模达数十亿美元的“货币独立王国”。围绕比特币的“铸造”、流通、兑换与支付，这一“货币独立王国”聚拢大量的利益相关者，构建了自己独特的权力契约，更打造出了日益成熟的生态圈。

比特币既非最早，亦非唯一的虚拟物品生态圈，游戏道具、虚拟币乃至电子优惠券都有自己的生态圈。但作为一类无机构控制、无第三方监管、可直接与法币双向流通、去中心化的货币，比特币与其他虚拟物品存在显著差别，因而其生态圈表现出完全不同的结构，内涵也更加丰富。

比特币流通链

从一个比特币生产、储存、流通、兑换、支付的完整过程出发，我们逐一分析每个环节涉及的各项服务、机构与利益，可对比特币流通链的构成形成一个全局性的认识。

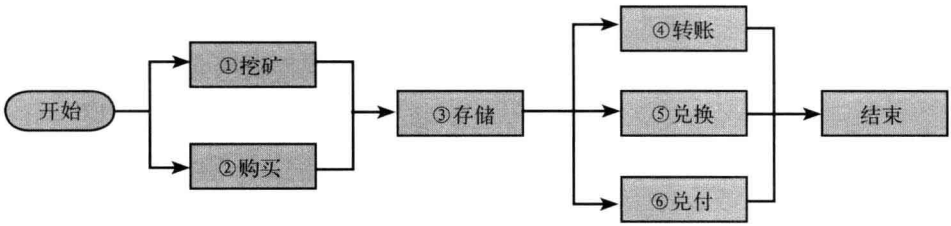

图 1　比特币操作流程图

图 1 是一个典型的比特币操作流程图，假设一个从未接触过比特币的新手要玩比特币，他首先需要了解如何获取比特币的问题。获取比特币的方法一般有 3 种：挖矿、购买以及接受他人的转账。挖矿需要拥有相应的软件与硬件，是一个庞大的产业链；购买要么通过线下进行，要么通过网上的交易所，也是一个庞大的产业链。

在获得比特币之后，要对比特币进行存储以便日后使用，这就涉及钱包问题。而使用比特币的途径无外乎 3 种：转账，即把自己的比特币直接转给他人；兑换，即把比特币兑换为法定货币（如美元、欧元、人民币等）或其他虚拟币，如莱特币（Litecoin）、XRP 币（Ripple 币）等；兑付，指转账与兑换的结合，即对于不接受比特币的交易方，可把比特币先转账给支持实时

兑换技术的第三方，然后由第三方把比特币实时兑换为交易方愿意接受的货币并完成支付。

需要强调的是，上述各个环节并非泾渭分明，相互之间经常有所交叉和重叠，但是这些环节均涉及大量的服务机构与人员，并由此构成了比特币生态圈的主体。

前提

无论是挖矿还是购买，在获得比特币之前，用户都需要先生成一个比特币地址，以便把得到的比特币转入该地址，真正获得所有权。而比特币地址需要通过特定的软件生成，因此下载一个比特币客户端是体验比特币的首要前提。比特币客户端一般由开源社区开发，并无偿提供给用户使用。这里涉及的主要实体就是比特币开源社区，由软件开发、测试人员组成，几乎没有直接的经济利益诉求，依靠分享和奉献精神支撑比特币体系的运行。

挖矿

挖矿是生产比特币的唯一途径，也是所有比特币的根本来源。它首先涉及挖矿软件，这些软件可直接从网上下载、安装，一般由开源社区或个体开发者提供，矿工可免费使用。

由于早期参与者少，全网算力很低，个人通过计算机的显卡甚至CPU（中央处理器）便可轻易挖到比特币。随着大量矿工的加入，全网算力持续

飙升，个人通过普通的计算机直接挖到比特币的概率急剧下降，目前几乎完全没有可能。这就催生了两个相关的产业：比特币矿机和矿池。

比特币矿机的目的是，针对挖矿算法进行硬件设计和优化，早期的矿机侧重于对多个显卡的支持，使得一台计算机可以提供尽可能高的GPU（图形处理器）运算能力。随着竞争的加剧，专用的挖矿芯片诞生，矿机的争夺已经深入计算机芯片设计与制造层面。而矿机产业也细化为两个子领域，一个是ASIC（专用集成电路）芯片的研制，一个是外围设备的配套与整合。矿机产业的成本较高，一般采用公司化机制运作，有的靠出售硬件获利，有的靠自产自用挖矿获利。其衍生产业为矿机租赁，通过向矿工出租矿机获利。

即使拥有了专用矿机，单个矿工或机构还是很难凭一己之力抢得比特币的记账权。因为在形式上，比特币的记账权每次只能被一个矿工获得，参与竞争的其他矿工则颗粒无收。因此，独立挖矿者的失败风险巨大而机会成本高企。为了改变这种局面，有人构建了比特币矿池，集中大量的矿工和设备共同挖矿。矿池的实质是把每次抢夺记账权的运算量依照算力分配至池中的各个计算机，这些计算机合并起来作为一个异常强大的“虚拟矿工”与池外的其他矿工或矿池争夺记账权，成功的概率大大提升。如果成功挖到比特币，矿池将依据事先约定的规则向各个矿工分配收益。矿池的创建者和维护者大多依靠手续费（每次成功挖掘后的抽成）获利，也有个别免费的矿池把挖到的比特币完全分配给矿工。

购买

直接向他人购买比特币是获得比特币最简单、最直接的方式，省去了挖矿的烦琐。购买少量比特币可以通过网上交易所（如Mt.Gox或Bitstamp等），这也是比特币生态圈最先商业化的一个环节，数量众多的交易所依靠收取交易手续费获利。每日通过交易所公开转手的比特币总量都在万枚以上。值得注意的是，通过交易所获得的比特币大都存储在交易所的账户里，如同银行的存款，只是数字而不是钞票。要真正获得这些比特币的所有权，用户需要通过交易所的提现功能把相应数量的比特币转移至自己的比特币地址上妥善保存。

如果要一次性购买成千上万个比特币，那么网上交易所并不是最佳途径，因为公开交易的市场容量有限，一次性购买额过大很可能会引起比特币价格飙升，进而给购买者带来不必要的经济损失。大额交易通常在线下进行，若购买者认识比特币的足量持有者，二人可商定价格和付款方式直接进行交易。通常情况下，购买者会选择找一个可靠中间人，向中间人表达购买意愿、数量与价格（此价格一般会略贵于当前公开的市场交易价），并约定付款方式（可能需要提前付款），中间人认可后向矿工或矿池发出购买邀约，矿工或矿池把此后一段时间内新挖到的比特币直接交付给购买者，或者交由中间人代转。中间人通过收取相应的手续费获利。

存储

比特币的官方客户端自带比特币存储功能，即“软件钱包”，也可通过

钱包备份功能把比特币备份在硬盘或其他存储设备上。为保障钱包的安全，一般推荐用户对备份文件进行加密。

由于软件钱包依赖于本地的存储介质，使用起来并不方便，因此部分网站（如Blockchain、Bips）提供了在线钱包功能。其实质是由网站代为维护你的钱包数据，便于你随时随地使用比特币。但是由于你所有的比特币信息都存储在网站上，对于在线钱包网站的选择需要慎之又慎，以免上当受骗。在线钱包一般是交易平台或比特币支付网站提供的附加功能，用户基本上都可以免费使用。

无论是软件钱包还是在线钱包，都存储着用户的公钥（比特币地址）和私钥，如果这些数据被损坏，同时用户又忘记了自己的公钥和私钥（事实上，除抄写下来外，用户几乎不可能记得那么长的字符串），那么钱包里的比特币就再也没有办法取回来了。为了避免这种情况，可以考虑使用之前介绍的比特币纸钱包和脑钱包。

转账

比特币官方客户端自带转账功能，但是由于比特币机制的设计，每次转账需要确认6次才能确保绝对安全，而每次确认需要等待10分钟，所以完整的6次确认最短也要花费一个小时，非常不便。尽管一些网站或者软件支持少于6次的确认，但所花时间仍然较长，比起当前接近实时到账的网银或第三方支付来说，速度成为其一大劣势，也严重影响使用体验。

为了解决这一问题，许多比特币支付公司提供了解决方案。其基本思路是用户把比特币充值进网站，由网站统一管理。例如用户A在某支付网站的账户中拥有20个比特币，他向同样拥有该网站账户的用户B转账10个比特币。网站验证用户A确实有10个以上的比特币“储蓄”后，就直接把A的比特币数量减去10个，把B账户里的比特币增加10个即可，中间根本不需要进行真实的比特币转账，因为A、B的比特币都由该网站托管，其道理与银行相同。这种转账服务一般作为比特币支付解决方案的一部分，由专门的商业化公司提供，公司收取相应的手续费作为自己的收入来源。

许多时候，转账的目的是支付，而支付是为了完成购买。比特币购物也是比特币生态圈里非常重要的一环，其线下运作形式类似于现金支付，线上运作形式则类似于电子商务，只是商家和用户都接受使用比特币进行交易罢了。而对于不接受比特币的商家，现在也有了妥善的解决方案，将在“兑付”环节详加说明。

兑换

兑换的方法和途径与购买类似。不过购买环节的兑换侧重于法币与比特币的兑换，而在此处，还可以指比特币与其他虚拟货币的兑换，如莱特币、XRP币等。这里涉及的实体机构同样是线上交易所，例如，Mt.Gox和Bitstamp主要支持法币与比特币的兑换，而BTC-e还支持比特币与多种虚拟货币之间的兑换。同样，这些交易所通过收取手续费获利。

兑付

兑付其实包含了两个环节，即兑换和支付，二者在时间上紧密连接在一起，共同完成一次交易。举个简单的例子，用户A想用比特币购买商家B的某件物品，而商家B不愿意接受比特币，那么用户A只能把比特币先兑换成法币，再把法币支付给商家B，这一过程相当繁琐，对于比特币的推广来说是个障碍。

为了解决这一问题，比特币支付公司可作为支付中介，使用程序把A的比特币实时兑换为法币后自动转账给B。这一过程对A、B均透明且灵活。如果A和B愿意使用同一种货币，支付中介直接转账即可；如果不愿意，支付中介先进行实时兑换然后支付。这种中介模式甚至超越了比特币支付的范畴，可在任意两种货币之间进行，操作简单，用户体验良好，因而颇受用户和商家的青睐，成为当前比特币生态圈中比较热门的领域。比特币支付公司同样通过收取交易手续费获利。

从上述介绍中，我们基本上已经可以获得比特币流通链的大致面貌。在流通链的货币“发行”环节，存在着矿机和矿池；围绕购买环节，则存在着交易所和中间人；各种钱包服务在比特币的存储方面发挥着重要作用；比特币支付服务和电子商务使得比特币走入现实世界，与实体物品建立联系；比特币基金会、开源社区、比特币信息服务和金融服务对整个生态起着重要的支持作用，所有这一切构成了比特币生态圈（见图2）。

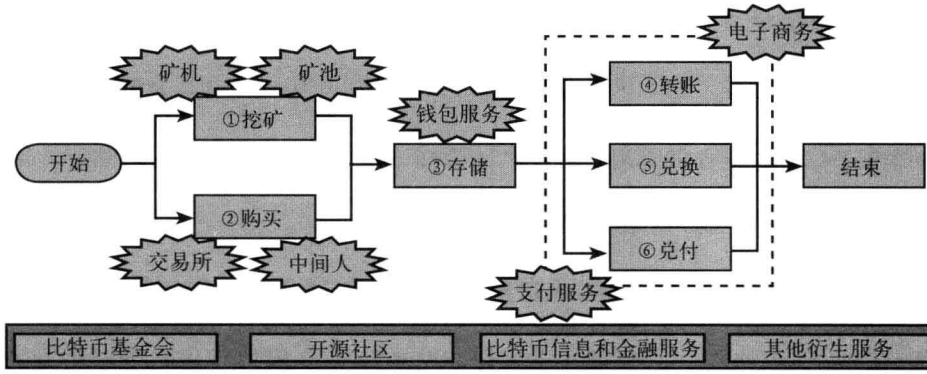

图 2　比特币生态圈

比特币基金会

比特币基金会成立于 2012 年 8 月，其目的是通过标准化、保护和推进开源协议，促进比特币的全球增长。作为一家非营利性公司和中立协作论坛，比特币基金会采用类似于Linux基金会和Tor（第二代洋葱路由匿名代理网络）项目的开源机构运作机制。具体而言，其主要任务包括：

标准化比特币：支持比特币基础设施的建设，包括赞助核心开发团队持续改进比特币软件来维持比特币的优异特性，使其得到更多的尊重、信任，提高接受度；

保护比特币：维护、改善并从法律上保护比特币协议的完整性；

推广比特币：作为比特币社区的意见表达渠道，宣讲比特币的技术与理念，澄清公众对比特币的误解、曲解和误传，提高比特币的声誉。

比特币基金会的成员分为3类：个人、企业和基金会创始人，目前由一个5人董事会管理。这5人的席位也相应的分为3类，其中2个席位来自个人成员，2个来自企业成员，1个来自创始人成员。按照基金会的章程，董事会每两年一届，期满后重新选举董事会成员。

目前，比特币基金会的企业成员有38个（包括2个白金会员和36个银牌会员），个人成员有500余人（包括200多位终身会员和300多位年费会员）。这些成员囊括了比特币生态圈的主要公司、机构和个人，具有广泛的代表性。入基金会需要缴纳相应的费用（这些费用必须用比特币支付），比特币基金会主要依靠会员费和捐助运作。

比特币基金会成立以来，在推广、保护、维护比特币方面不遗余力，例如不定期发布比特币软件更新通知、征集比特币技术/项目提案、召开比特币大会、在各种会议上宣传比特币、对某些比特币事件进行评价和回应等。由于这些努力，比特币基金会在比特币社区中享有很高的声誉，被称为比特币的“半官方”机构。

该基金会近期比较著名的两件事当推2013年5月底美国加州的禁止令事件、8月与美国联邦政府的对话。已在第一章有过详细介绍，此处不再赘述。

比特币交易所

由于比特币尚未被广泛接受，还不能在现实世界中自由使用，所以那些拥有比特币的人经常希望能把比特币兑换成法币，获得“摸得着”的财富；而许多爱好者想拥有比特币却又不想挖矿，用法币购买比特币便成为自然诉

求。有需求、有供给，比特币交易所便应运而生，目前已发展成比特币世界的重要一环，是联系比特币虚拟世界与法币现实世界的桥梁。当前国外著名的比特币交易所有Mt.Gox、Bitstamp和BTC-e等。

Mt.Gox

作为最负盛名、最大的比特币交易所，Mt.Gox于2010年7月17日在日本成立，当时的比特币价格每个还不到5美分。由于成立较早，Mt.Gox发展得很快，其交易量一度占据全球线上比特币交易总量的80%以上，在比特币的兑换方面几乎具有决定性的力量，是整个比特币市场的风向标。而比特币历史上的几次价格暴跌也都与Mt.Gox大有关联。

2011年6月19日，Mt.Gox上出现了令人震惊的超低卖出价，一分钟内，比特币价格从每个17美元跌至每个10美元，几分钟后甚至狂跌至每个0.013 4美元。最终结果是，26.1万个比特币以每个1美分的价格成交。虽然30分钟后比特币的价格重回每个13美元，但是此事严重打击了比特币参与者的信心，比特币的价格随之一路走低，到当年11月份曾一度跌至每个2美元。这一事件的原因是一个拥有大量比特币的Mt.Gox账户被黑客攻破，Mt.Gox为此事歇业一周。

2013年，比特币最引人瞩目的暴跌当属4月11日，那一天下跌近60%。据Mt.Gox官方解释，起因是比特币的交易过于活跃、新用户数量增加过快使得交易系统不堪重负而出现延迟。而这一情况被用户误认为是黑客攻击，因

而引发恐慌性抛售并最终导致价格暴跌。Mt.Gox为此暂停交易12个小时。

Mt.Gox平台的功能纯粹、操作简单，主要包括如下功能：

交易：该功能又包含交易（买卖比特币）、资金选项（对账户进行充值或提现）、账号历史（可以查看自己的充值、提现和交易记录）、结账按钮（为商家生成“结账”按钮，便于比特币支付）。

商家工具：主要供商家使用，一般用户用不到该功能。

安全中心：主要帮助用户增强账户的安全性，用户可以在这里添加自己的YubiKey（一种身份认证的硬件）或者软件认证器，然后选择登录、提现和进入安全中心时所愿意使用的附加安全措施。

设置：用户可在此设置一些个性化信息、修改密码或申请认证。Mt.Gox的用户身份分为未验证、已验证和受信3种。如果想向账户充值或提现，用户必须向Mt.Gox提交相关材料，获得已验证或受信身份。

常见问题：该功能连接Mt.Gox的客户支持和论坛，用户可以在这里查看常见问题，也可以向客服提交服务请求。值得注意的是，由于Mt.Gox的客户支持与论坛采用同一账户系统，用户提交请求后，需要重新注册一个论坛账号方能查看自己的请求与客服的回复。

新闻：Mt.Gox的官方新闻区。

作为第一大比特币交易商，Mt.Gox在2013年经历了严酷的监管压力。3月，美国财政部下属的FinCEN要求为比特币或其他虚拟货币提供经纪或转

账服务的业务必须进行注册，意在对比特币交易进行监管。5 月，美国国土安全局获得法院的许可，冻结了Mt.Gox的两个银行账户，查封资金超过 290 万美元。国土安全局通告称查封的原因是Mt.Gox的首席执行官马克 · 卡佩勒斯没有如实告知这两个银行账户的用途是货币兑换。此外，Mt.Gox的网络支付平台Dwolla也因受到影响而关闭。6 月初，FinCEN再次重申比特币交易需要遵守的规则，继续对Mt.Gox施压。

与此同时，Mt.Gox与其战略合作伙伴CoinLab（比特币孵化器公司）闹翻，CoinLab宣称Mt.Gox违反了一项赋予CoinLab北美市场独占权的合同条款，并且不允许他们按合同约定将现有的美国、加拿大客户从Mt.Gox转移到CoinLab。CoinLab要求赔偿 7 500 万美元的经济损失。在内外交迫的情况下，Mt.Gox不得不采取务实策略，于 6 月 26 日向FinCEN提交注册申请，该申请于 6 月 28 日被批准，Mt.Gox获得MSB牌照，终于走上了“合法化”的道路。

Bitstamp

位于斯洛文尼亚的Bitstamp是第二大比特币交易所，成立于 2011 年 8 月。Bitstamp的特点是比特币的价格一般比Mt.Gox略低（10%左右），手续费也稍低一些——Mt.Gox的初始交易手续费为 0.6%，Bitstamp为 0.5%。因此对于要购买比特币的人来说，在Bitstamp上交易比Mt.Gox要划算；而对于出售比特币的人来说，其提现也较Mt.Gox方便。凭借这些差异性优势，Bitstamp逐渐发展壮大。

Bitstamp平台的功能也比较简单、直接，包括：

概览：主要展示当前的市场交易情况和Bitstamp近期新闻。

账户：包括与账户余额、交易、未完成订单、安全、设置、支持、验证账户、账户历史有关的全部功能。

买/卖：主要用于比特币交易，但用户也可以在这里购买XRP币，只是Bitstamp的XRP币价格比Ripple官网高，购买时需谨慎。

订单簿：展示当前的比特币市场深度信息和所有买家、卖家的出价信息。

充值：从外部银行、平台或钱包把比特币、XRP币或现金充入Bitstamp平台的用户账户。

提现：把Bitstamp平台用户账户中的比特币、XRP币或现金提取至外部银行、平台或钱包。

Bitstamp比Mt.Gox多了一项购买XRP币的功能（只能买不能卖），事实上它也是Ripple网络的最大网关。由于Ripple网络本身并不提供充值、提现功能，用户在Ripple网络上进行支付或交易时，需要先把比特币、XRP币或美元转入一个网关，然后把网关里的钱再转入Ripple网络（除XRP币外，这些货币并未真正转入Ripple网络，只是在记账形式上有所变化）。Ripple网络上比特币、XRP币、美元三者之间的兑换，Bitstamp网关占到了90%以上的份额。

作为比特币兑换界的第二大商家，Bitstamp一直与Mt.Gox明争暗斗。事实上二者近期就上演出了一场比特币价格的激烈暗战。2013年6~7月，

Mt.Gox为配合FinCEN的注册工作，暂时关闭了提现通道，此举再次引起用户的恐慌，导致比特币价格持续下跌。作为风向标的Mt.Gox比特币价格自然影响到Bitstamp，其平台上的价格也随之下跌。但与此同时，Bitstamp竭力阻止比特币价格下跌，希望能够尽量缩小二者的价差，甚至期待超过Mt.Gox比特币的价格，以便吸引Mt.Gox平台上的比特币持有者转到自家平台上进行交易，进而一举击溃Mt.Gox。

二者的价格曾一度非常接近，但随着两周后Mt.Gox重新开放提现通道，比特币社区的恐慌情绪释放完毕，比特币的价格又开始稳步攀升，二者之间的价差亦再次拉开。经过这次较量，Bitstamp虽未能击败Mt.Gox，却也明显削弱了后者的优势。目前，这两个平台每日比特币交易量的对比已经不如之前那么夸张，一般处于1 ： 1~2 ： 1之间（之前可达3 ： 1~4 ： 1甚至更高）。

尽管Bitstamp近期的发展势头良好，但Mt.Gox被美国政府强制注册之后，Bitstamp很可能会面临类似的监管压力。Bitstamp也明智地在6月份关闭了美元的代码充值和转让通道（这一通道不透明、难以追踪，容易滋生洗钱、偷漏税等违法交易）。由于它在美国没有银行账号，开户行在欧洲，交易使用的法币又主要是美元，等于同时给美国和欧洲的货币监管当局出了难题。

BTC-e

BTC-e也是一家老牌虚拟货币兑换所，由俄罗斯人开办，其特点是兼收并蓄，支持的虚拟货币种类很多，一度是莱特币的头号交易平台，在比特币

兑换方面也有一定的地位。由于其交易手续费低、入金（充值）/出金（提现）便利，自由主义气氛比较浓厚，常被视为冒险家的乐园，许多新型的山寨币都以能上BTC-e交易平台为荣。

目前可在BTC-e上交易的虚拟货币包括比特币、莱特币、域名币、NVC（Novacoin）、TRC（Terracoin）、PPC（PPcoin）和FTC（FeatherCoin）等，种类全面。但是与Mt.Gox和Bitstamp的单一性相比，BTC-e由于对山寨币过于开放，而用户又很难了解某个新型山寨币的来龙去脉，因此需要承受一定的风险。在BTC-e平台上曾多次出现某个新虚拟币上架，欺骗了一些用户之后，又被下架的情况——用户的损失当然无人负责。

此外，BTC-e的安全问题也曾受到诟病。例如，2012年2月，有人就发出警报称BTC-e存在严重漏洞；2012年7月，BTC-e被黑客攻破，大约损失了4500个比特币，BTC-e不得不暂停交易并赔偿用户的损失。而用户密码被破解、虚拟币被盗的事件在BTC-e平台上也时有耳闻。因此，普通用户在BTC-e上交易山寨币时需要格外小心，避免陷入骗局或者成为黑客的打劫目标。

矿池与矿机

矿池的作用是汇集零散、独立的计算资源，通过统一软件的调度，对挖矿的计算量进行拆分和分配，形成一个强大的虚拟矿工，增加单个矿工的稳定收益，降低失败风险。矿工的收益则在矿池抢到记账权后，根据特定的规则进行分配。

由于全网算力的增加和矿池的兴起，现在单个矿工想通过独立挖矿获得

比特币已经几乎不可能，加入矿池、按照自己的贡献度获取比特币已经成为矿工的唯一选择。当前比较著名的矿池有Deepbit、BTC Guild等。

Deepbit

Deepbit是一个老牌矿池，以稳定性著称。在Deepbit挖矿的步骤如下：

1. 在Deepbit网站上注册账户。

2. 登录网站，填写比特币钱包地址，设置挖矿设备（Worker）。

3. 下载比特币挖矿软件。

4. 启动挖矿软件。

5. 在挖矿软件中创建采矿器，服务器选择Deepbit，并按照Deepbit上填写的挖矿设备信息输入电子邮箱和密码。

6. 开动矿机，等待收益。

Deepbit的特点为：

采用长轮询机制通知挖矿设备有关新区块的信息，降低过期贡献的数目（可减少0.5%~1.5%）。

只要抢到记账权就给矿工分成，即使该区块后来被废弃（0.5%~1.2%的概率）。

挖矿设备无响应时会给矿工发电子邮件。

矿工可随时点击“即时支付”按钮拿走自己的收益。

矿工可选择两种支付模式：按次付费——挖矿软件每提交一个计算结果，就得到固定数额的比特币。此方式的收入是固定的，但是费用较高，因为矿池承担了长时间挖不出比特币的风险。如果矿工期望稳定的收益，可以选择此模式。

按比例付费——每挖到一个比特币块，就会按照某矿工的计算量占挖到该比特币块所需总计算量的比例分配比特币给该矿工。此种分配方式获得的收益是变化的，因为挖到比特币所需的时间是随机的。

具有竞争力的价格：按次付费，每次向矿工支付 0.000 000 342 205 010 14 个比特币；按比例付费只收取不到 3%的手续费。

即时分账，无须等待。

公开、免费注册，不限制用户或连接的数目。

BTC Guild

BTC Guild是目前最大的矿池，计算能力超过 150TH/s，估计很快会达到200TH/s。使用BTC Guild矿池挖矿的步骤与Deepbit类似：

1. 在BTC Guild网站上注册账号。

2. 注册完成并登录成功后，设置电子邮件、时区、监控挖矿状态、团队、钱包地址等。

3. 在网站上创建挖矿设备，有几个GPU核心就需要创建几个挖矿设备。

4. 启动挖矿软件。

5. 在挖矿软件中创建采矿器，选择BTC Guild服务器，并按照BTC Guild上填写的挖矿设备信息输入名字和密码。

6. 开动矿机，等待收益。

BTC Guild的支付模式也分两种：一种与Deepbit相同，即按次付费，现在矿工每次可获得的收益为0.000 000 351 710 705 7，略高于Deepbit的0.000 000 342 205 010 14；另一种则称为按最后N次付费。后者的计算比较复杂：首先，把所有用户提交的计算次数打包分为一组，每组称为一个轮次，目前每个轮次大约由9 000万个计算次数组成。一个轮次完成后，该轮次被称为开放轮次。依次完成10个轮次后，这10个里面最早的轮次就关闭了。

在一个轮次处于开放状态时，矿池发现的任何区块的收益将支付给所有开放的轮次（共10个，每个轮次均分收益的10%），这意味着即使一个矿工暂停挖矿，它依然可以从尚未关闭的轮次中获得收益。

每个轮次支付的收益=（（区块价值+交易手续费）/10）-矿池费用（3%）

这个收益再均分给在该轮次中提交的约9 000万个计算次数。当然，按最后N次付费方式的收益也是不固定的。如果矿池的运气好，抢到的区块多，矿工就会挣得多一些。从长期来看，例如按照几个月的跨度计算，矿工选择这种模式会比按次付费多挣约5%。

Slush矿池

Slush是比特币历史上的第一个大型矿池，产出一般但很稳定。其使用方式与其他矿池相同，支付模式则杜绝平均主义，严格按照算力贡献比例分配收益，上一轮的收益不会带入下一轮，只有参与抢得记账权轮次里的矿工才有资格获得收益。

Slush矿池收取的手续费较低（2%），此外还有一些独特之处：

诚实劳动、终身服务：用户需要相信矿池管理员，因为如果管理员使坏的话，矿池根本无法防范。Slush矿池自2010年12月以来持续运行，拥有长期的稳定而精确支付的历史。

支持Stratum协议：该挖矿协议专为高速ASIC（专用集成电路）矿工设计，网络开销极小。

基于分数的回报系统：矿池采用公平的收益分配方案，已从数学上证明了这可以防止矿池的剧烈波动。

其他矿池还有50BTC、烤猫等，选择矿池除了考虑稳定性、收益、手续费这些问题之外，一定要注意矿池的诚实度，因为矿池完全有办法把集体挖到的比特币多分给自己一些，甚至可能欺骗矿工、独占收益。因此，诚实、可靠应该是矿池的首要品质，否则矿工连被骗了都不知道，即使知道也很难讨回自己的应得收益，因为比特币世界的一切都依靠信任和算力，没有强制执行手段。

与此同时，由于矿池汇聚大量的计算资源，形成了强大的算力，在处处

依靠算力投票的比特币世界里，矿池俨然是一个个“封疆大吏”，在比特币事务上拥有一定的发言权和影响力。2013 年 3 月，比特币 0.7 版和 0.8 版客户端因区块大小限制的不同而导致不兼容，互不承认对方的有效性，比特币网络面临分裂的危险局面。比特币社区发出警报后，几大矿池迅速响应社区的呼吁，将客户端切换到了旧版本，在短短几个小时内便化解了这次危机。可以说，这次事件在一定程度上考验了矿池，也可视为一次算力民主的胜利。

矿机是专为比特币挖矿设计和优化的硬件，目的是大幅增强挖矿设备的计算能力，使矿工在记账权的激烈争夺中占据有利地位。比较著名的矿机有阿瓦隆、ASICME、烤猫和蝴蝶矿机。

阿瓦隆矿机

早在 2011 年下半年，国内的南瓜张就推出了第一代FPGA（现场可编程门阵列）矿机，单卡速度高达 360MH/s，售价为每台为 600 美元，超过GPU速度数倍。该矿机引起轰动，供不应求，南瓜张也因此一举成名。经过两个月的优化，第二批FPGA矿机的单卡速度提升至 400MH/s，售价降为每台 569 美元（如果要进行二次开发，还需购买 69 美元的开发套件）。

FPGA矿机实际上是一种电脑外设，据南瓜张介绍：电脑上的程序申请任务，用串口发给FPGA，FPGA内部的控制模块把这个任务转给运算核心，这个运算核心的哈希能力就是理论速度。FPGA最大的优势是便于集群，可

以用一台电脑连接几十个FPGA矿机，达到每秒几G甚至几十G哈希的运算速度，这在当时绝对是运算神器。

FPGA矿机极大地提高了运算速度，但是由于其功耗较高，速度的进一步提升面临瓶颈。因此，矿机界纷纷把目光投向了ASIC技术，开始研制ASIC芯片。南瓜张也与时俱进，转向ASIC芯片的研发，并于2013年1月交付首台阿瓦隆矿机，该矿机每模组的运算能力高达66GH/s。阿瓦隆矿机共销售3个批次。

由于ASIC芯片设计与生产的成本高昂，而外设的匹配耗费的资源更高，并不利于充分发挥阿瓦隆团队的核心优势。因此，阿瓦隆团队在成功推出矿机之后宣布转型，开源除阿瓦隆芯片以外的硬件解决方案，不再出售组装好的矿机，转而成为专门的芯片研制与供应商。其一代芯片采用100纳米的制作工艺，二代芯片拟采用55纳米工艺，本预计2013年年底开始销售，但截至目前，传来的只有跳票的消息。

烤猫矿机

作为一家深圳的比特币挖矿公司，烤猫长期占据世界冠军的宝座。2012年8月，烤猫通过众筹模式筹集到约10万美元，当年年底制造出矿机的芯片样品，其矿机主要用于自家挖矿。目前，烤猫矿机的算力占据整网算力的20%~30%，实力强大。

2013年4月16日，烤猫对外公开发售矿机，率先拍卖第一批10台刀片

挖矿机，最终成交价为每台 75 个比特币。5 月 4 日，又发布USB矿机并在全球销售，10 000 多台很快就被一抢而空。5 月 13 日，烤猫又宣布面向全球销售刀片矿机，市场反应良好，截至 7 月初的销量已超过 500 台。

烤猫的刀片矿机分为两种：一种算力为 10GH/s，功耗在 70W 左右；另一种迷你型的算力为 5GH/s，功耗减半。这两种矿机可以自由组合，再配上电源和风扇，可以组成算力更强大的矿机。8 月份，烤猫启动新一轮刀片矿机的销售，价格为 3.5 个比特币，7 个小时后全部卖完。

烤猫矿机最大的优势在于只卖现货，省却用户等待的时间和风险，但是普遍认为其定价较高。

蝴蝶矿机

蝴蝶实验室是一家美国的矿机研制机构，其最大特点是雷声大、雨点小，产品跳票严重。

在FPGA时代，蝴蝶实验室就开始研制比特币矿机，除 2012 年年初个别美国矿工收到过蝴蝶FPGA矿机（算力约为 820MH/s）外，就再无音讯。在阿瓦隆和烤猫发布ASIC矿机之后，蝴蝶实验室也宣称要推出ASIC矿机，而且首批产品就打算采用 65 纳米工艺，瞬间在业内引起轰动，名声大噪。

然而，蝴蝶矿机从 2012 年 6 月开始接受预订，整整过了一年，少量预订者才收到他们的 5G矿机，所有被预订的 5G矿机何时能发货完毕还是个

未知数，至于100G、500G等大机器的订单就更是遥遥无期。2013年8月，蝴蝶实验室又推出了采用28纳米工艺的600G矿机，声称发货日期为2013年11月或12月，价格为4 680美元。这批矿机能否如期交付、会跳票多久仍有待观察。

随着挖矿设备的持续升级，大量专用矿机投入市场，尤其是ASIC矿机的出现，意味着普通用户依靠CPU或GPU已经基本上不可能挖到比特币了。据估算，目前矿机提供的算力已经达到整网算力的90%以上。而作为矿工，要继续从事挖矿这份有前途的事业，购买专业矿机已是必然选择。但是，由于比特币矿机多为期货，交货周期动辄数月，矿工在购买矿机前一定要预测未来的算力增长情况，仔细测算投资收益比。否则，很有可能陷入矿机一入手就开始赔钱，进而永远无法收回成本的困境。

比特币支付

比特币被誉为“未来的世界货币”，而作为货币，它必须与现实世界的物品挂钩，即只有可以使用比特币购买商品时，才算切实而完整地履行了自己的货币职能。但是采用比特币支付，还存在一些严重障碍，例如：由于确认机制的制约，比特币无法实时到账；由于币值波动较大，许多商家虽然认可比特币的价值，却不愿接受比特币支付。这就需要专业的比特币支付公司来解决这些问题，开辟便捷、顺畅的比特币支付渠道。

BitInstant

BitInstant是一家位于纽约的初创公司，它首先是一个比特币交易商，提供买卖比特币的在线平台。截至2013年5月，它拥有16名雇员，其首席执行官查尔斯·谢尔梅宣称，随着比特币价格的上扬，2013年公司的交易量增长迅速，4月甚至增加了2倍，超过110万美元。

与一般的交易所不同，BitInstant事实上是一个交易中介，主要是为其他比特币交易所提供便捷的充值和提现渠道。例如，2012年4月19日，BitInstant和Coinapult交易平台合作为用户提供通过电子邮件发送比特币的服务，其过程如下：

1. 用户通过其他电子钱包向BitInstant账户充值，并选择电子邮件为接收方式。

2. 系统立刻购买对应数量的比特币（收取少量费用），并经由Coinapult通过邮件发送。

3. 用户收到电子邮件后就可以提取这些比特币或者随意发送。

这个功能对刚接触比特币的人特别有用，他们不用自己在比特币交易所里交易，只需向BitInstant充值，由BitInstant代为购买即可。

2012年9月，当时的美国总统候选人米特·罗姆尼收到一封威胁邮件，要求他必须向某个匿名组织支付价值100万美元的比特币。BitInstant的埃里克·沃里斯帮助米特·罗姆尼购买了比特币，并且免除了手续费，BitInstant由此名声大噪。

2013 年 3 月,BitInstant遭到黑客攻击。黑客先是控制了该公司的DNS（域名系统）服务器，进而控制了邮件服务器，并经由对以上系统的控制成功登录另一家比特币交易公司VirWox，最终盗走了价值 12 480 美元的比特币。

2013 年 5 月，BitInstant获得文克莱沃斯兄弟 150 万美元的投资。2013 年 6 月，BitInstant宣布与在线支付公司Jumio合作，BitInstant可使用Jumio的专用软件验证用户的身份。同年 7 月，BitInstant暂停服务，宣称正在对网站进行改版以便引入新功能和新变化，当时其用户大约有 17 300 人。截至 8 月底，该网站仍未恢复。

BitPay

BitPay成立于 2011 年 5 月，是一家专注于比特币支付的初创公司，其目标是做比特币界的Paypal。BitPay主要面向商户提供比特币支付方案。假如一个商户需要接收一笔付款，而消费者只想支付比特币，那么商户就可以在自己的网站上设置BitPay的比特币支付按钮。消费者点此按钮支付比特币，BitPay接收比特币，然后向商户的账户里打入兑换后的法币。这对于跨国交易尤其方便，省却了外汇兑换以及汇款的烦琐，也节省了高昂的手续费。

对于商户来说，通过BitPay的技术方案完成比特币支付，可为消费者额外提供一种结算方式，并且能够解决某些信用卡结算时常出现的问题。BitPay的大多数商户来自美国，其次是英国、加拿大、澳大利亚、芬兰。共有 98 个国家的商户使用BitPay处理比特币付款，这些商户以电子商务店铺

为主，辐射零售、数字内容、慈善、独立承包人、移动支付等多个领域。因为接受比特币付款，BitPay降低了互联网付款的成本和风险。因此，与竞争商户相比，相同商品在BitPay的价格要便宜1%~2%。如果使用比特币，付款就像发送电子邮件一样方便，同时不需要通过银行、政府或公司审核。

Coinbase

Coinbase由Airbnb（房屋短期租赁网站）的创始人布雷恩·阿姆斯特朗于2012年6月创建，并由大名鼎鼎的创业孵化器Y Combinator扶持，其目的与BitPay类似，也是提供便捷的比特币购买与支付服务，是比特币支付界的一家酷公司。

Coinbase通过众筹获得了618 700美元的投资。2012年年底，Coinbase宣布美国用户可直接通过银行账户买卖比特币。到2013年年初，用户在Coinbase上的交易额超过100万美元；到5月，其交易额更是达到1 500万美元。

2013年5月，Coinbase获得了500万美元的A轮融资，由国际顶级创业投资基金联合广场领投，成为第一个完成A轮融资的比特币公司。

2013年7月，Coinbase推出即时支付服务，用户无须等待银行转账的延迟，即买即付。据悉，该服务最高限额为50个比特币，而且只对完全认证用户开放。

2013年8月，Coinbase宣布准备开始支持比特币离线小额支付，并且可以在Coinbase系统中瞬间完成。比特币经济学家蒂尔·德梅斯泰表示，Coinbase的这项举动非常创新，能够促进比特币生态圈的健康发展，也有助

于加快比特币的流通速度。同月，Coinbase又创建了一个短信界面，使用户可以通过短信发送和接收比特币。随后，Coinbase宣布对商家前100万美元收款免收手续费，以促进比特币支付。100万美元之后，手续费为1%，基本上与其竞争对手BitPay 0.99%的手续费持平。

比特币金融

货币必然会衍生出金融，对于比特币来说同样如此。小到一个项目，如果该项目受到玩家的认可，而项目负责人自己又没有足够的资金操作该项目，他就可以通过比特币社区进行众筹融资，利用融到的比特币支撑项目运作；大到一个公司，为了开展新业务、筹集资金，它可以发布以比特币为入股货币的招股书，并进行首次公开募股。目前，若干公司已经走上了比特币首次公开募股的道路，而网上的比特币股票交易所也已初见雏形。

比特币首次公开募股

这其中最典型的公司要算烤猫了。为筹集ASIC矿机的启动资金，烤猫团队于2012年8月份在GLBSE交易所（现已关闭）进行了首次公开募股。首次公开募股的总股本为40万股，其中的50%由比特泉（bitfountain，烤猫的官方名称）持有，发行价为每股0.1比特币。最终售出了16万~17万股，以当时的汇率计算，筹得了约100万元人民币。借助这笔启动资金，烤猫团

队成功独立研发并量产ASIC矿机，并从2013年4月开始出售现货USB矿机及刀片矿机。

目前烤猫的股票主要分为3类：

1.直接股：100%分红，直接以比特币钱包地址登记，每个地址对应一定的股份数量。分红时，烤猫会直接把比特币发到相应的钱包地址。

2.转手股：通常是由交易网站的运营者购买直接股，然后以相同数额在交易网站上进行交易。由于其分红需要经过转手，故称为转手股。

3.拆细股（1股拆细股=烤猫股份的1%，分红时通常要扣除5%手续费）：由于烤猫股价一路走高，目前已经在4.3比特币左右，对于小散户来讲，并不容易凑齐这么多比特币。有人看到了其中的商机，开发出了将烤猫股票拆分为100份的品种。每一股相当于直接股的1%。这些拆细股只能收到95%的分红，5%当作管理费被扣除。

烤猫股票自2013年2月28日开始分红，每周三分红一次，分红的金额波动较大，最低为每股0.002 6比特币，最高为每股0.038比特币。

比特币股票交易所

当前比较著名的比特币股票交易所包括BTC-CT和BitFunder。二者的共同点是操作简单、安全性较好。二者支持的股票均为40只左右（包括直接股、转手股和拆细股）。

此外还有Havelock Investments，注册地位于加拿大，特点是界面较商业化，同时提供IPO信息。MPex是交易所中的技术派，网站用户界面交互性好、交易量大，适合大量交易或技术派人员使用，安全性很高。

在这些交易所里买卖股票与普通的股票交易所类似。用户先在网站上注册，充值后选择自己心仪的股票，给出报价即可，只是所有的交易都通过比特币进行。

比特币其他金融品

比特币是虚拟世界的货币，而任何货币都将不可避免地衍生出金融服务。这其中最引人注目、实践上也相对充分的是比特币众筹模式。同时比特币生态圈也呈现出其他金融应用形态。

据传全球第一家比特币银行已经秘密开张，其运作模式与传统银行相同：吸收用户的比特币存款，然后把存款贷给那些需要比特币的人。比特币银行主要通过收取存款与贷款之间的息差获利。

2012年，国内还成立了首家比特币对冲基金，主要通过比特币交易获利。该基金的净值在不到一年的时间里，已经涨了10倍。但从2013年2季度开始，由于比特币市值波动过大，该基金已解散。

第一章也提到，2013年7月初，美国的文克莱沃斯兄弟已正式向美国证监会提交首次公开募集申请，计划创办一个史无前例的基金——比特币交易型开放式指数基金。

今年4月，美国的Coinsetter公司融资50万美元，计划打造一个比特币的外汇交易市场，向比特币市场引入杠杆和卖空交易。

而据坊间消息，在法律允许的国家开设比特币赌场的项目计划书，已经摆在某些风险投资人的案头。其实，在此之前，一些网络上的赌博小游戏早就使用比特币作为筹码了。

这些交易方式在成熟市场上很普遍，但是在比特币市场上还比较少见，其竞争对手有Bitfinex和ICBIT等交易平台。此外还有提供比特币借款服务的Coinlenders，比特币投资基金Ultima Fund，比特币P2P借贷平台BTCjam，比特币二元期权交易平台anyoption等。

比特币作为虚拟货币，其核心不在于虚拟，而在于货币。货币的累积构成资本，而资本自身具有保值、增值的特点，比特币金融市场必然诞生，而且势必会不断发展壮大。但值得注意的是，无论何种类型的金融市场都存在风险。当前，由于人们对比特币的热情高涨，比特币社区弥漫着过度乐观的氛围，相关的风险正在累积，需要引起比特币爱好者的充分关注。无论是对于股票、借贷还是期权，投资都有风险，入市需谨慎。

激进实践

在比特币新手看来，比特币无非是挖矿、买卖而已，是一个软件和一个交易所就可以搞定的事情。而事实绝非如此，在这些简单的行为背后蕴藏着整个庞大的比特币生态圈。

第一，比特币网络需要有专人维护，这一网络依靠比特币客户端和挖矿软件构建，这就涉及软件开发者，以及对这些开发者给予支持、组织和协调的组织（如比特币基金会）。

第二，挖矿软件依靠硬件设备运行，矿工们会想方设法提高自己的收益、降低风险，矿池和矿机产业应运而生。

第三，除了把比特币兑换为法币的需求外，部分持有者还希望充分发挥比特币在支付方面的优势，直接使用比特币购买物品，比特币支付公司在此过程中起到重要作用，成为联系用户与商家的桥梁，也促进了比特币经济规模的扩大。

第四，比特币成为货币之后，持有人有投资、增值的愿望，其他人有融资、借款的需求，两者结合就诞生了比特币金融市场，并激发出衍生品。

第五，比特币理念的推广与普及离不开论坛、博客等信息服务平台，这些平台帮助入门者理解比特币，手把手地教他们挖矿、搬砖、投资，为比特币生态圈的繁荣也做出了巨大贡献。

比特币作为一次伟大的货币实验，涉及的人数超乎我们的想象，其中有些人是比特币信念的狂热支持者和奉献者；有些人则更多的是出于好奇而随行就市；还有人充满投机目的，只是为了赚一票就走。无论参与者的动机是什么，这些人实际上都参与了比特币生态圈的构建，而这一初具雏形的生态圈则为比特币的去虚拟化奠定了坚实的基础，是所有参与者共同的贡献。

其中意义最深远的是，比特币通过构建自己的生态圈展现了社会契约重构的一个鲜活案例。自由本位的货币（包括目前所有的法币）本质上是一纸

契约，政府低成本印出的每张钞票代表着它与持有者签订的一份价值合同，这个合同名义上以政府的信用为担保，实质上以政府的强制力执行，因而是一种强制契约。个体既无选择的余地，亦无对抗的能力。19 世纪欧文的乌托邦理念试图把民众从政府的强制契约中解放出来，其思路是让所有人都变成好人，从而消除监管的基石。结果是他失败了。

而在比特币的世界里，几乎一切都依赖于算力投票：比特币的增加靠算力投票获得，比特币的安全传输靠计算机投票保障，比特币交易的不可欺骗、不可撤销也靠算力投票达成，甚至比特币规则的更改、客户端的完善都靠算力投票选择。仅仅依靠算力投票，去中心化的比特币网络竟然神奇地存续了下来，而且持续发展壮大。其中的关键在于，算力背后是一个个矿工和用户，他们用计算设备直接为对自己最有利的行为投票，一个GPU一票，公平合理，童叟无欺。这里面没有代议制，没有法官和警察。因而，比特币网络实际上完成了一场大范围直接民主的激进实践，打造了一个货币自治的乌托邦：每个人依靠自己的直接投票权建立起一种新型的P2P契约。这种契约在零信任的前提下达成，好人没有额外回报，坏人的伎俩也无从施展。依托这种理论上极其不稳定、实践上却极其有效的P2P契约，比特币网络的发展出乎每个人的意料。

这或许是许多高智商极客热爱比特币的真正原因，也可能是比特币给我们上的最深刻的一课。把这种思路扩展至金融、经济领域，我们或许可以确定的说：真正的互联网金融和互联网经济还远远没有到来。

05 挑战与破解之道

笔者曾在一个比特币的QQ群里担任管理员，群里大部分是刚入门的比特币者，对于比特币的原理一知半解，连中本聪的论文译本都没完整读过。这些人却往往一出手就买上几十上百个比特币，即使按照当时的价格，也相当于人民币几万到几十万元。他们无一例外的对于比特币的未来充满了信心。

在比特币的官方论坛上有各种不同的观点、意见，其中对比特币持长期悲观态度的人不在少数。一般来说，知道这个论坛且在上面发言的网友对比特币的认识已比较深入，他们非常清楚比特币存在的问题，并且认为这些问题最终会毁掉比特币。

那么，比特币是否会因为这些问题而最终消亡呢？比特币的确存在很多缺点，但相较于传统货币和其他虚拟货币，这些缺点实在是微不足道，远不足以毁掉比特币。

在本书出版之时，比特币可能又经历了一次过山车行情，价格到达一个新低点，市场上会再次弥漫着“比特币已死”的论调，而比特币的各种问题也被夸张地呈现在公众面前。那时候，请你记得我以上的判断以及200多年前雨果说过的一句话：

世界上最强大的力量莫过于应运而生的思想。

比特币的常见问题

比特币交易全过程

首先，讲一个关于比特币交易的故事。从这个故事里，我们可以了解比特币交易的流程，以及流程中各个步骤存在的问题。

有一天，长人在网上闲逛的时候发现了一家网店，里面的商品新潮有趣，而最重要的是，它支持比特币支付。作为比特币的坚定信仰者，他与店主聊得非常投机，决定以10个比特币的价格购买一件商品。出于对店主的信任，长人与店主约定，由前者将10个比特币打到后者的地址上，而后者在收到比特币后再将商品发出。

店主打开自己的比特币钱包，创建了一个新的比特币地址，并告知长人。店主创建新地址的本质是生成了一个密钥对，这个密钥对由一个公钥和一个私钥组成，其中私钥只有店主自己知道，而公钥则是公开的，可以用来验证支付的真伪。

长人收到店主的地址信息后，打开了自己的比特币钱包客户端，并指示客户端将 10 个比特币发送到店主的收款地址。钱包客户端里储存着长人所有地址的私钥，为了简化问题，我们假设长人在其中一个地址里放了 11 个比特币，而本次支付只从该地址进行扣款。在发送比特币时，钱包客户端以该地址的私钥对本次交易进行签名，并向全网公布这次交易信息。

这个时候，网上所有的节点或者说每一个矿工都会验证这个交易是否有效。验证方法也很简单，拿出这个地址的公钥对照即可。在这个环节，名叫宋欢平和睡空空的两位矿工也接到了这个交易信息。在经过验证确认交易有效后，他们把这个交易放进内存里，等待进入数据块。过了一段时间，宋欢平的电脑算出了一个符合条件的随机值，系统宣布一个新的合格数据块诞生，并向整个网络公布了这一消息，其他节点（包括睡空空）收到后就开始在这个数据块之后开始新的挖矿工作。而长人和店主的交易信息就被打包放进了宋欢平挖出的数据块里，并且得到了初步确认。当下一个区块链接到这个区块时，交易就会得到进一步的确认。在连续得到 6 个区块的确认之后，长人和店主的这笔交易基本上就不可逆转地得到了确认。

店主发现 10 个比特币已经到达他的地址，经过一段时间的等待确认后，他把商品发给了长人，本次交易宣告完成。

确认时间的问题

在这个故事里，最引人注目的问题在于比特币的确认时间。宋欢平和其

他矿工不断地测试以得到符合条件的随机值，而求得随机值所需的时间已被系统预先限定，平均耗时 10 分钟。也就是说，无论矿工们多么努力，挖出一个数据块所需要的时间总是在 10 分钟左右。如果要保证交易的不可逆转，则要等待 6 个数据块完全确认，这至少需要 1 个小时的确认时间。

为什么比特币交易需要确认呢？这涉及双重支付的问题。如果长人给店主支付 10 个比特币的同时，未等系统确认，又用同一个地址（内有 11 个比特币）向其他地址支付了 10 个比特币，并且采取了一些技术手段（比如将 10 个比特币分散成极小份发送到若干地址里，使得系统优先确认该项交易），使得后一笔交易优先于前一笔得到确认，那么店主最终将得不到那 10 个比特币。简单来说，一笔比特币交易的等待时间越久，得到的确认越多，它就越安全。

如果这种交易发生在网络上，且销售对象不是时效性非常强的商品，那么等待 1 个小时的确认时间也无所谓。但如果是在日常生活中，比如在商店里，那确认时间就成问题了。我们很难想象，上班前在 7–11 里用比特币付款买了糯米鸡当早餐的白领，要在店里等上 60 分钟才能离开——在迟到 5 分钟就要扣奖金的今天，这有点儿不切实际。

这个问题的本质其实是信任。你是否信任与你交易的人，这是解决问题的关键。为了便于分析，我们拆分成以下几种情况进行讨论。

/熟人交易/

这里的熟人不一定是朋友，可能是楼下商店的老板。他每天都能看到你

上下班，见面了还会打招呼，你也经常去他店里买东西。在这种情况下，他不会太在意确认时间，因为你已经是熟客了，不太可能为了贪小便宜而把自己的信誉丢掉。

/陌生人的大宗商品交易/

在陌生人进行初次交易时，彼此的信任难以马上建立。在这种情况下，确认时间是必要的，但不一定是不可接受的。想象你去 4S（以“四位一体”为核心的汽车特许经营模式）店买汽车，当你用比特币支付完毕后，店员同时为你的新车办理各种手续。这种大宗商品交易所需的手续时间通常比比特币的确认时间长得多。那么，交易双方通常都不会太介意交易的时间确认问题。

/陌生人的小额交易/

这是比特币目前遇到的最大的技术难题。在一个大城市里，很多小额交易是发生在陌生人之间的。比如你走进街边的星巴克，点一杯咖啡带走。在这种情况下，服务员不认识你，而你也不可能为了一杯咖啡等上 10 分钟甚至 30 分钟。如果比特币的确认时间一直停留在目前阶段，那么这确实是一个问题。

2013 年，在美国圣何塞召开的比特币大会上，与会者提出了很多解决理念。其中最重要的一个叫作链外交易，即不在区块链内进行交易确认。假如有一家公司能以其一贯良好的信誉赢得用户的信任，从而推出自己的在线钱

包软件，那么只要星巴克及其顾客都注册了该公司的账户，顾客们便可以把自己的部分比特币存入该公司账户，并通过在线钱包购买星巴克等企业的商品，将比特币从自己的账户汇入星巴克的账户。由于这种交易实际上只是在该公司的系统内部进行账内金额转移，不涉及区块链的确认，所以交易几乎是在瞬间完成的。这种方法能够解决陌生人之间小额交易的确认问题。

钱包的安全问题

在长人和店主的交易中，两人都使用了比特币钱包客户端。大部分用户都会选择Bitcoin-QT等客户端作为自己的比特币钱包，储存私钥。钱包在比特币使用过程中的作用至关重要。但事实上，比特币的使用风险大多集中在钱包上：

误把钱包文件删除以至于丢失价值数万美元的比特币；

没有正确备份钱包文件，导致一段时间内交易的比特币全部丢失；

电脑中了木马病毒，钱包文件被盗，所有比特币荡然无存。

以上种种问题都是钱包客户端的特性造成的。

/官方钱包客户端的风险/

首先要说明的是，所有的钱包客户端里面都没有比特币。从比特币的特性可知，它其实是流动在网上的一本大账本里面的数字。而比特币钱包里面存放的是用户的私钥，主要用来证明该用户对账本里的某个数字拥有所有

权。每当用户要动用自己的比特币财产时，便动用钱包里某个地址的私钥进行签名，以向全网广播，证明地址里的比特币归他所有。

以官方钱包客户端Bitcoin-QT为例。该客户端存放比特币私钥的文件是Wallet.dat，一般Win8系统下的存放路径是C:\Users\电脑的用户名\Appdata\Roaming\BitCoin（需要注意的是，一般Appdata是隐藏文件夹，需要修改系统设置使隐藏文件可见才能找到）。Wallet.dat的本质是一个私钥池，存放的是这个钱包的所有地址的私钥。有了这个文件，用户才能证明自己对钱包地址里的比特币的所有权。钱包风险其实可以分为以下几种情况。

一是，Wallet.dat文件被偷。这是最常见的钱包风险。如果用户的电脑被黑客入侵，Wallet.dat文件被黑客获取，那么黑客也同样对钱包里的地址拥有支配权。在用户尚未察觉之前，黑客就会把该地址所能支配的比特币统统转移。

二是，Wallet.dat文件丢失。这种情况并不少见。在未做好备份的情况下，误删了Wallet.dat文件，则用户所有的比特币都会丢失。与Wallet.dat被盗不同的是，在这种情况下，这些比特币从此只会在网络上如孤魂野鬼般游荡，不归任何人所有，因为唯一证明所有权的私钥已经永远消失。这些丢失的比特币会使现有的比特币总量变少。

三是，Walllet.dat备份出错。比特币钱包客户端的设置使得Wallet.dat文件的备份成为一个技术活，稍有不慎就会造成严重损失。

在初始状态下，Wallet.dat的私钥池里存有100个私钥。当“生成”一

个新地址时，客户端其实并没有真的产生一个新地址和对应的私钥，而只是从私钥池里取出一个使用，同时再生成一个（真正意义上的）新的私钥和地址并放进私钥池里，使未使用的私钥数量保持在 100 个。

而使问题变得更复杂的是客户端本身的找零机制设置。依照比特币本身的规则，一个地址上的比特币在支付的时候必须全部支出，除向另一个地址支付比特币外，剩余金额再重新支付给原地址（见图 3）。

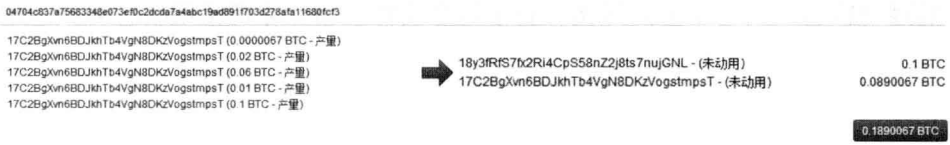

图 3　交易示意图

17C 的地址里之前有 0.189 006 7 个比特币，当 17C 的拥有者发出向 18y 的地址支付 0.1 个比特币的指令后，系统会将 17C 地址里的 0.189 006 7 个比特币全部取出，并将其中的 0.1 个比特币转入 18y 的地址里，剩余的 0.089 006 7 个比特币重新打回 17C。

而客户端出于保护用户匿名性的考虑，并不会将余额打回原地址，而是从私钥池里取出一个新地址并将余额打进去。在缺省设置下，这个地址并不会显示在客户端的界面里。

所以，用户每进行一次交易，私钥池里原有的私钥就被取出一个，同时又有新的私钥补充进去。如果用户对 Wallet.dat 进行备份之后完成了 100 次交易，那么私钥池里的原有的全部私钥就都用完了，接下来使用的都是未曾备

份的新私钥。使用新私钥完成交易之后，如果用户用原来的备份文件进行恢复，那么所有未备份的新私钥都会丢失，而这些新地址里的比特币也会随之丢失。

/解决方法：增加钱包安全/

就增强钱包的安全性而言，以下几种方法颇为有效：

一是，离线钱包。私钥的功能在于证明自己拥有某个地址里的比特币的所有权，其作用方式是对交易单进行签名，根本不需要放在联网的电脑里。离线钱包应运而生，这是储存比特币最安全可靠的方法。

关于离线钱包的使用方法，网上已有完整的教程，搜索“Armory离线钱包教学”即可找到。其主要原理是，将私钥放置在一台永不联网的电脑里，将钱包存放比特币的地址放置在联网的电脑里。由于联网的电脑没有私钥，所有交易单在联网电脑里下单后，需通过U盘（移动存储设备）拿到离线的电脑上进行私钥签名，再拿回联网的电脑进行全网广播并确认交易。存放私钥的电脑全程都不会接触到网络，所以可以保证私钥的绝对安全。

二是，纸钱包和脑钱包。所谓纸钱包，其实就是把私钥印在纸张上。纸钱包的好处显而易见：实物的纸张远比U盘或硬盘可靠，可以有效躲避黑客的盗取。主要缺点就是使用的时候，需要先用客户端导入私钥。纸钱包主要适合储存大额的、近期不打算使用的比特币。

脑钱包的产生机制则是从比特币地址和公私钥的算法推导出来的。根据

比特币的算法，通过任何一个单词或短语都可以产生一对独一无二的公私钥和比特币地址。所以，用户只需要记住随意一句话，便可以通过这句话导出一个专门的比特币地址和私钥。这句话就是所谓的脑钱包。

如果使用得当，纸钱包和脑钱包的安全系数都非常高，但还有要注意的地方。

一是，脑钱包密码的复杂度。因为银行等机构的关系，人们习惯了4~6位的密码。他们想当然地认为脑钱包的密码也只需6位数即可，但他们错了。银行和网站有专门的系统来保护用户资料，不允许黑客多次尝试密码；而比特币的所有地址都在网上公开可查。黑客可以不断试错，直至找到对应的私钥。那么，找到一个6位密码对应的私钥需要多久呢？密码应该使用数字、大小写字母和符号，那么每一个密码的可能性有95种字符（26个大写字母、26个小写字母、10个数字、33个符号），6位密码的组合有A（95，6），即大约8.6亿种可能性。这个数字看起来似乎很大，但实际上一台普通的计算机用2.5分钟就可以遍历全部结果。

从理论上说，8位数以上的包含95种字符的密码应该是安全的，因为按照目前的计算机速度，暴力穷举法对8位以上的密码基本上无能为力。但问题是，人脑很难想出一个完全随机的8位密码。我们能想到的密码总是跟我们日常思维习惯有着千丝万缕的关系，黑客们一般都有一本密码词典，上面记载了各种可能的密码组合。通过这种方法，破解一个8位的普通密码通常只需要几分钟时间。

如果你觉得自己想出来的密码足够复杂、可靠，不妨先来看看以下被黑客破解出来的密码：

k1araj0hns0n

Sh1a-labe0uf

Apr!1221973

Qbesancon321

DG091101%

所以，依靠人脑想出一个可靠的脑钱包密码的难度非常高。相对安全的脑钱包密码的要求是：足够长，40 位或以上，防止被暴力穷举法破解；别人不容易猜到；对你来说，很容易记得。

一种比较好的方法是“掺盐”，即在原有用户密码的基础上加入一个随机密码。很多网页都有生成随机密码的功能。用户可以首先生成一个 20 位的随机密码，将该密码用各种方式保存下来（比如，文本打印、加密压缩并进行云存储等），然后将该密码与原有密码组合在一起，生成一个新的脑钱包密码。这样一来，该账户基本可以说是安全了。即使黑客破解了你的常用密码或者随机密码，他也无法轻易获得你的脑钱包密码。

另一个好方法则是从电子书里选一段你最喜欢的话。比如，我很喜欢林达的《西班牙旅行笔记》，决定用书里第 35 页的第三段作为我的脑钱包密码，那么我要记得的就是本书第 35 页第三段这一信息而已，而任何人几乎都无法猜到我这种带有强烈个人特点的脑钱包密码。

二是，找零机制的注意事项。纸钱包和脑钱包在存储比特币方面表现一流，但在支付时却有些麻烦。如果选择用Blockchain客户端，将纸钱包或脑钱包的地址放在上面，那么支付时就可以直接输入私钥并调用这些资金。但对于有强烈安全需求的人来说，一旦一个私钥在网上被输入过，那么这个对应的地址就不再安全了。因此，除非是需要动用钱包里的全部资金，一般来说不推荐在Blockchain客户端导入私钥进行支付。

另一种方法是使用Bitcoin-QT等钱包客户端。导入私钥后，纸钱包或脑钱包里的钱就成了你钱包客户端里的一部分，使用方法跟平常并没有什么区别。但由于之前提过的找零机制的存在，纸钱包或脑钱包导入私钥并完成一次支付后，原来钱包里的比特币余额将全部转移到客户端的另一个隐藏地址。如果需要将其重新放回钱包，还需要再进行一次支付，将余额打回原来的地址。曾经有用户在通过客户端导入脑钱包私钥完成支付后，随手将客户端的Wallet.dat文件删除，导致余额全部消失，损失巨大。

区块链的内容合法问题

在之前的故事里，长人和店主都会将全部区块链信息下载到自己的本地硬盘里并及时更新区块链信息。但区块链里有时不仅存有交易信息，还存在其他一些奇怪的、可能违反当地法律的内容。

这似乎并不算什么问题，但在很多国家，这是一个严肃的法律问题。

比特币交易里是允许嵌入一小段信息的，比如一段话或一段代码，但之

前曾有用户将一张儿童的色情图片的代码上传到了区块链里，只要通过一定的解码软件，这段代码就可以转换成图片。

问题来了：在很多国家，在知情的情况下以任何形式保有儿童色情图片都是违法的。比特币当下的属性决定了每一个用户都必须把全部区块链信息都下载到自己的电脑里，那么实质上，每个比特币用户都以某种形式存放了一些违禁内容。设想如果上传的色情内容足够耸人听闻，那么比特币用户很难辩称自己并不知道区块链内有违禁信息。对于立法者来说，这是一个无法回避且必须认真面对的问题。

SHA-256 被破解了怎么办

整个比特币的安全核心在于SHA-256 安全散列演算法。根据维基百科的定义，SHA-256 及其他SHA 算法能计算出一个数字信息所对应的长度固定的字符串。输入的信息不同，对应的字符串也极有可能不相同。SHA-256 被称作安全算法，主要基于以下两点：第一，由信息摘要反推原输入信息，从计算理论上来说是很困难的。第二，想要找到两组不同的信息对应到相同的信息摘要，从计算理论上来说也是很困难的。任何对输入信息的变动都极有可能导致其产生的信息摘要迥异。

在整个比特币交易过程中，有几个地方会使用到SHA-256 算法，其中最重要的莫过于挖矿。一笔交易要经矿工们确认有效后才能放入区块进行全网广播，而区块的产生则是一个寻找随机数以计算特定散列值的过程。矿工们

在挖矿时需要依靠强大的算力不断尝试，平均耗时 10 分钟才能找到该随机数。这个所谓的工作量证明的机制保证了无人可伪造或重复任何交易。

如果SHA-256 算法被破解，那么攻击者可以从两组不同的信息推出相同的信息摘要。也就是说，他可在极短的时间内找到该随机数，从而快速产生区块。在这种情况下，基于工作量证明的比特币安全机制也就形同虚设了。

不过，最严重的后果并不太可能发生。首先要说明的是，SHA-256 算法目前被公认为最难破解的算法之一，因此也被银行、军队等对安全度要求极高的机构采用。如果SHA-256 被破解，那么首当其冲的绝对不是比特币。

而当前网上对于SHA-256 算法可能被破解的担忧，主要来自于此前MD5 被破解一事。2004 年，山东大学教授王小云公布了MD5 的破解报告。需要说明的是，这一报告只是证明存在一种可以产生强特定碰撞的方法，但要伪造数字签名则必须能够产生弱特定碰撞。因此，MD5 实际上并没有被真正破解，更不用说比MD5 安全度更高的SHA-256 了。担心SHA-256 被破解而引致比特币的毁灭实属杞人忧天。

不过，探讨一下在遥远的将来SHA-256 被破解的可能性，也是一件有趣的事情。如果SHA-256 真的被破解，姑且不论这事会对银行和军事安全产生什么影响，单就比特币社区而言，会产生什么后果？

事实上，中本聪早已回复过这个问题。2010 年 6 月 14 日，他在比特币官方论坛的一个帖子里分两种情形进行了讨论：一种是SHA-256 被突然宣布破解成功，在这种情况下，比特币社区的大部分用户可以决定，在某个

区块之前的所有区块属于“诚实”区块并予以承认，在该区块以后重新使用新算法挖矿。另一种情况则是SHA-256没有被突然破解，而只是发现了隐患，因此转换可以逐步进行。使用新算法的客户端将被提前开发，并约定在某一个区块之后开始实行，所有用户将在该区块被开采出来之前更新客户端。

从以往的经验来看，大部分加密算法都是逐步发现漏洞，并在一段较长的时间内被其他算法替代的。因此，最有可能发生的情形是，比特币采用的SHA-256算法在未来5~10年内开始发现能产生强特定碰撞的方法，并被宣布为不安全算法，而比特币社区也因此从某个时间段开始统一使用新算法的客户端，实现平稳过渡。

如果遭遇51%攻击怎么办

51%攻击是从比特币成立的那天起就有人担心的问题。在比特币体系中，交易信息存储在区块链里。长人和店主的新交易放在了宋欢平新开采出的区块里，而这个区块则位于之前最长的那条区块链的末端。一般来说，区块链都是一串直线的连续区块组合，但在一些特殊情形下，区块链会产生“分叉”，即在区块链的末端出现了两个互相冲突的区块。在这个例子里，我们假设一个区块里包含的交易信息是长人支付了10个比特币给店主；而在另一个区块里，交易信息则是长人将10个比特币发给了他自己的另一个地址。当冲突区块出现时，比特币网络将投票决定哪一个交易是有效的，投票方法就是

每一个矿工在其认为有效的区块后继续开采新区块，而最终最长的那条区块链将被认定是唯一有效的。

如果长人足够聪明，也有足够的算力，他就会将支付给店主的比特币同时支付给自己。而因为他的算力超过了50%，从长远来看，他能够比其他人更快地找到开采区块需要的那个随机数，因此，长人实际上拥有了决定哪一个区块有效的权力。

当一个攻击者控制了全网50%以上的算力，从他掌握控制权的那一刻起，他能够：

修改自己的交易记录，这可以使他进行双重支付。

阻止区块确认部分或者全部交易。

阻止部分或全部矿工开采到任何有效的区块。

他无法做到的是：

修改其他人的交易记录。

阻止交易被发出去（交易会被发出，只是显示0个确认而已）。

改变每个区块产生的比特币数量。

凭空产生比特币。

把不属于他的比特币发送给自己或其他人。

无论从哪个角度看，51%攻击已经不算比特币的一个大问题了。

第一，51%攻击是比特币世界最古老也最著名的攻击方式，每个人都在关注，而且知道相应的应对措施。

第二，矿机的出现使得比特币挖矿的算力获得了大幅提升。在当前超过100T的算力下，任何个人或机构都几乎不可能制造51%攻击。

综合上述情形，潜在的51%攻击只可能来自于某个政府机构，集全国之力秘密造出一台超级计算机，以期击溃比特币，挽救自己的货币发行体系。但这依然是不太可能发生的事。并非所有政府都天然对比特币怀有敌意，即使某个政府拥有了51%攻击的能力，它会发现使用该能力进行挖矿便可垄断比特币的发行权，其收益远远大于击溃比特币，攻击动机也就不复存在。

山寨币会取代比特币吗

比特币是一种开源的P2P货币，基本没有技术门槛。因此，在比特币成名后不久，大量仿制品问世，试图在密码学货币市场中寻得一席之地。这些仿制品在圈子内被称为山寨币。那么，有朝一日，比特币是否会被一种新的、更好的山寨币取代？

山寨币本身各有特点：有的对比特币的算法进行了改良（如莱特币）；有的则是纯粹的模仿，只求短期套利（如中国币）。在这里，我选择两种具有代表性的山寨币进行说明。

支付网络Ripple及其XRP币理念

/什么是Ripple/

在日常生活中，熟人之间互相借钱，可能并不会打欠条。有时几位朋友互相借钱，还可能视亲疏远近，尽量调整相互间的债务（权）关系。比如长人原欠宋欢平4元，宋欢平又欠睡空空4元。由于长人和睡空空比较熟，3人一商量，很可能就直接让长人还钱给睡空空。其实不光是熟人之间，即使对很多店铺来说，还会允许熟客赊账。

也就是说，每个人都更乐意跟自己信任或熟悉的人有债务（权）关系。通过人与人之间的信任网络，资金在其中顺畅地流动。

这是发生在现实世界的人与人之间的金钱网络。假如这一切发生在互联网世界呢？这就是Ripple试图在互联网中实现的货币流动体系。

Ripple是一个开放的支付网络。而在网络中，你和你信任的朋友的关系转换为你与信任的网关之间的关系。网关就是网络与现实世界的接口，犹如银行柜台，将你的人民币现金转换成你账户里的一串数字；也好比是拉卡拉充值点，将你存在银行里的钱转成支付宝里的金额。

当你通过信任的A网关将100元人民币换成A网关发行的CMY（设想的一种货币单位）后，你的Ripple账户里就会多出100CMY的金额，你可以将这100CMY通过网关转给一个陌生人埃米，而埃米则可通过A网关将这笔钱换成现实世界的人民币取出来。在整个过程中，债务（权）的变化情况如下：

1. 你将100元存入A网关，A网关欠你100元人民币，并给了你一张100CMY的借条；

2. 你将100CMY的借条通过A网关传递给了埃米，此时A网关不再欠你的钱，而欠埃米100元人民币，埃米则持有了A网关的100CMY的借条；

3. 埃米通过A网关将借条兑现成100元人民币。

整个流程中，你跟埃米都只是分别与A网关建立了信任关系，而你和埃米之间不需要建立信任关系。

/XRP币的作用/

那么，XRP币是用来做什么的呢？其主要功能是用来支付交易费用。

XRP币本身是内嵌在Ripple系统里的一种加密货币。与比特币不一样的是，Ripple在创立的时候就发行了1 000亿XRP币，且总额将不再增加，也就是说，它是一种预挖矿的货币。每笔交易（比如你将100CMY转给了埃米）都需要支付少量的XRP币，而支付的这部分XRP币将被直接销毁。同时，XRP币还被用来当作保证金，当你开设一个Ripple账户时，需要在里面放置50个XRP币。

Ripple的发行与维护公司OpenCoin表示，在1 000亿个XRP币中，200亿个会给予投资人和创始人；在剩下的800亿个里面，500亿个会被免费派发给大众（即在一段时间内开设账户是免费的），另外的300亿将由OpenCoin持有，不定时地抛售以获得利润。OpenCoin坦承，持有及抛售XRP币是其赢利的唯一途径。

/Ripple能否取代比特币呢/

Ripple诞生之初，传言四起。很多人声称，Ripple更符合现实中货币的运作方式，未来必将取代比特币。

但事实上，现在判断Ripple体系能否成功尚为时过早。Ripple刚刚开始运作，很多问题已经暴露出来，包括其安全性并没有官方宣传的那么好。

而且，Ripple本身是一个新兴的货币流通体系，而XRP币的本质则是协助体系内货币流通的润滑剂。如果这个体系有朝一日成功了，也只会对比特币的流通产生正面影响。说Ripple能取代比特币，其实就相当于说，支付宝能够取代人民币一样：一个是支付体系，另一个是货币，两者并不是同一类东西，没有可替换性。支付宝的出现为人民币的支付和流动提供了便利。同样，Ripple体系如果成功，其作用也只是促进比特币的支付和流通。

莱特币

/什么是莱特币/

莱特币是2011年10月7日发布的、目前市值最高的山寨币。和比特币相比，莱特币具有如下特点：

1.速度更快。莱特币的生成速度是平均2.5分钟一个块，比比特币快3倍，15分钟就可以完成6次确认。这是为了方便商户交易而设定的。

2.总量是比特币的4倍。莱特币的生成总数为8 400万枚。

3.采用Scrypt算法。

这是莱特币与其他纯粹模仿的山寨币最大的不同之处。Scrypt算法的最大特点就是，在运算中不能单靠CPU的算力，而需要大量的内存支持。目前，市面上的专业比特币矿机在莱特币挖矿方面都没有显卡挖矿有优势，因此，莱特币目前的矿工大部分都是依靠显卡挖矿。莱特币的发明者认为，这种设定可以让莱特币的挖矿权分散在大量散户手中，而不是像比特币那样，逐渐集中、垄断在大型矿机的拥有者手中。但需要指出的是，这种设置是一把双刃剑，在避免挖矿成为少数人参与的资本密集型产业的同时，显卡挖矿导致的总算力偏低问题也使莱特币相较于比特币更易遭受51%攻击。

/莱特币会取代比特币吗/

在比特币发明之后不久，怀疑的声音就已层出不穷。其中的一个就是，发行密码学货币没有门槛，任何人都可以发行山寨币。这些山寨币的通行最终势必会取代比特币，导致密码学货币的通货膨胀，最终摧毁比特币和其他密码学货币。所以，对于每一种山寨币的出现，都有人问：它能够取代比特币吗？

这个问题其实包含两个小问题：该山寨币能成功吗？该山寨币能取代比特币吗？

目前对于莱特币的一个观点是，它最终将存活下来并成为比特币之外的辅助货币。莱特币官网有一句著名的口号：“比特币是金，莱特币是银。”

另一种观点从逻辑角度论证莱特币和其他山寨币不可能成功：如果山寨币成功的话，就会出现更多山寨币，而山寨币泛滥将导致价值崩溃，人们最

终发现还是比特币保值；如果山寨币不成功，那么将不会有模仿者，失败的山寨币也会最终消失。

笔者倾向于认为，密码学货币最终将成为世界主流货币的重要成员，而其中不一定只有比特币，就像现实生活中美元、欧元、日元、人民币共存一样。密码学货币不会只有一种，但也不会有无数种共同存在于世界上，最终将只有比特币和另外 2~3 种山寨币能够存活下来。

实际上，最终取决一种开源货币是否能存活下来的关键是大众对它的信心，而信心来自长期而稳定的使用。莱特币从发明到现在的两年时间里，正在逐步建立公众对其的信心。这个信心能否维持下去，目前还有很多不稳定的因素，其中一个就是莱特币相对于比特币，更容易遭受 51%攻击。之前，与莱特币采用同样算法的FTC（羽毛币）已遭受 51%攻击，并导致公众信心的崩溃，FTC实际上正逐步退出历史舞台。能否抵挡 51%攻击并存活下去，是莱特币必须解决的问题。

而对于莱特币能否取代比特币这个问题，也许应该更进一步：有没有一种山寨币能够最终取代比特币？答案很简单：不能。

将来的世界很可能存在多种密码学货币，但任何一种山寨币都取代不了比特币的主流地位，无论它的算法与比特币相比是多么优秀。

我们必须承认，与很多山寨币相比，比特币并不完美。它的确认时间长达 10 分钟，对于交易来讲确实耗时长；51%攻击这把达摩克利斯之剑一直悬在头顶；从环境保护的角度来说，挖矿耗费的能源几乎白白浪费了。因此，很多新出现的山寨币都声称自己的优势就在于弥补比特币的缺陷。

但是，比特币本身的缺陷有一部分并不是真正的缺陷。或者说，这些缺陷是其发明人在权衡利弊之后刻意保留下来的，比如51%攻击的根源在于比特币这种P2P货币本身的分布式挖矿特点。而Ripple的XRP币倒不必担心51%攻击的问题，也无须耗费大量的能源进行挖矿，但其依赖信任网关进行交易及中心化发行货币的模式意味着，它极易被政府机构控制。

此外，即使有些山寨币的设计确实更加巧妙，我们也要了解一个事实：一个产品，无论其各方面的指标多么优秀，都不能保证它能击败竞争对手，获得成功。

我们在现实生活中能够见到很多例子。许多最早开发的产品并不完美，但却一直占据行业的主流地位。最好的例子莫过于我们日常使用的QWERTY键盘。研究表明，使用这种键盘进行文字输入的效率非常低下。比如，大多数打字员惯用右手，但使用QWERTY时，57%的工作是由左手承担的；两小指及左无名指是最没力气的指头，却需要频频使用；排在中列的字母的使用率仅占整个打字工作的30%左右，因此为了输出一个字，时常要上下移动指头。事实上，QWERTY键盘的设计本身就是为了降低打字员的打字速度，因为就早期的打字机而言，如果打字速度过快，很容易卡键。这种设计可以将常用的组合字母分散在键盘的各个角落，有效放慢了敲键速度。时至今日，卡键的问题早已不复存在，而这种效率低下的键盘设计却保留了下来。无论后来者提出的新设计方案多么高效，都无法取代QWERTY键盘的绝对主导地位。

这个例子的背后就是著名的路径依赖理论，即人类社会中的技术演进类似于物理学中的惯性，一旦进入某一路径就可能对这种路径产生依赖。和QWERTY键盘一样，比特币目前也进入了某种依赖路径，这使得其他山寨币难以有取代它的机会。比特币发展至今，已有大量的人力成本和时间成本投入在各种相关应用上。这就意味着，转向另一种密码学货币的转向成本会越来越大。而且当用户已习惯使用比特币之后，由于人性中普遍的安于现状、不愿改变的心理，很难因为其他山寨币的小创新而放弃比特币。

路径依赖理论确实也存在例外的情况，比如此前的相机胶卷。在爱迪生时代，胶卷的画幅被定义为24mm×36mm。后来的人们提出了各种新方案，试图重新定义胶卷画幅，但都徒劳无功，因为全世界使用旧有规格胶卷的相机保有量实在是太大了，人们不可能为了节省几毫米的胶片而扔掉自己价值上万元的相机。直到数码相机的发明重新定义了摄影，新的画幅标准才被普遍接受。这似乎表明，能够取代比特币的不是任何一种山寨币，而是另外一种划时代的创造。这种创造不一定跟货币有关，但其必然是某种能够为人类社会的运行方式带来革命性改变的东西，以至于在这种创造面前，任何货币都已失去了存在的必要。显然，目前来看，任何一种山寨币都难以担此重任。

从当下的情况看，要断言密码学货币在未来会成为主流货币似乎还为时过早，尽管其发展前景一片光明。然而，假设10年后密码学货币果真与美元、人民币一道，跻身世界主要货币行列，那么我们可以肯定的是，笑到最后的肯定是比特币。

如果政府宣布比特币违法怎么办

政府会打击比特币吗

从比特币发明之日起就有人宣称，比特币在未来必将遭到各国政府的打压，并被宣布为非法货币。其依据是，比特币的进一步发展将会威胁传统货币的利益，而统治者不会把权力拱手让给密码学货币。

一旦各国政府宣布比特币非法，其价格在短期内会产生剧烈波动，甚至可能崩盘。同时，政府会强制关闭比特币交易平台，那么比特币就只能私下流通变现，其兑现能力必将遭受严重打击。

政府究竟会不会取缔比特币？这个问题几乎是所有比特币持有者最担心的问题，就像永远悬挂在头顶的达摩克利斯之剑，你不知道什么时候比特币就因被政府宣布违法而一夜之间变成了废“纸”。这种恐慌一直无法消除，所以经常看到某些相关的负面新闻被过度解读，比如Mt.Gox的某个外汇账户被关闭，市场就谣传成首席执行官被捕。因此，这是一个所有比特币爱好者必须要面对的问题，应该予以高度重视。

但即使很多人都有这个担忧，却很少有人真正去深入思考，包括：政府为什么要打压比特币？政府依靠什么手段来打压比特币？

并非所有政府都有这个动机

政府打压论的理论基础在于，认为货币是政府控制权力的有效工具，因

此政府定会将货币发行权牢牢掌握在自己手里。然而，世界上很多国家，包括美国，都允许私人发行货币。2006 年，在美国的马萨诸塞州伯克希尔区域，就有一家私人公司发行过一种私人货币——BerkShares 币。这种货币在伯克希尔区域流通，目前已有 370 多家商户接受这种货币。BerkShares 币的汇率与美元保持同步，但也有学者认为，应该将汇率与当地商品的价值挂钩，以免美国经济的波动影响到当地的经济发展。

因此，并不是全世界的政府都有天然的动力去打压私人发行的货币。退一步说，即使有一些国家的政府决心控制货币发行权，禁止任何私人货币在本国流通，但要从技术上取缔比特币是几乎不可能完成的任务。

法律与技术障碍

仅从操作层面讲，目前世界上没有任何一个政府拥有通过法律来限制一个公民记住两串字符串（公钥和私钥）的权力。而且，从技术角度讲，关闭一个 P2P 网络根本就不是人力所能完成的事。P2P 本身的性质决定了，一个项目一旦启动，就无法被关闭。

对于 51% 攻击的问题，前面已经分析过，即使某个政府拥有了 51% 攻击的能力，它会发现使用该能力进行挖矿便可垄断比特币的发行权，其收益远远大于击溃比特币，攻击动机也就不复存在。

可以想象，在这种情况下，任何一个政府要废除比特币，所面临的困难都是极大的。

因此，比特币存在的关键不在于政府是否封杀它，而在于爱好者们是否能一直保持对它的信任，只要信任存在，比特币仍然有价值，仍然无法阻止人们使用它来兑换法币或交换物品。

大而不倒

2008 年的金融危机让人们都熟悉了一句话：大而不倒。这是指一个金融系统越庞大，它就越有保障。因为越大越有价值，越有价值，倒闭的破坏力越大，使得连政府都不得不想方设法阻止它的倒闭。对于比特币系统来说，也是同样的道理。它的稳定程度取决于是否有足够数量的公民财产及足够多的公司财团进入这一领域。进入系统的财富越多，政府封禁时要面临的阻力越大，甚至不得不估量封禁后的严重后果。

从 2013 年 4 月以来，风险资金积极涌入比特币创业领域，说明部分资本已经开始向比特币系统倾斜。同时值得高兴的是，比特币最活跃的国家——美国，对于比特币一直持比较开放包容的态度。正如FinCEN所说：我们对虚拟货币并无成见，只希望比特币能够接受适当的监管，以便打击洗钱、非法交易等同样存在于法币世界中的违法行为。

德国政府则通过法律，判定持有比特币一年以上者免收增值税。也就是说，德国认为比特币并不违法。

事实上，由于比特币本身跨国境的性质，世界上只要还有一个政府不禁止比特币，比特币消亡一说便无从谈起。在比特币尚处于发展的早期阶段，

已有两个重要的国家（美国和德国）给予其肯定的态度。这或许可以使我们对比特币面临的未来政策风险少一些不必要的担心。

自律自强

前面从国家以及法律与技术难点的角度分析了比特币被封禁的可能性，并得出了乐观的结论。然而这些都是外因，比特币能否持续发展壮大、茁壮成长，更多的是基于内因，包括它是否有价值，是否被用到了正确的地方。否则外因再有利，比特币自身无价值或比特币社区不自律，比特币也无法获得光明前景。

对于比特币的价值，在前面我们已经长篇累牍地进行了讨论，在后面的章节中还会继续深入探讨。而在自律自强方面，现状也正朝着对比特币有利的方向发展。世界上最大的比特币交易所Mt.Gox已向FinCEN提出注册申请，获得了MSB牌照。Bitstamp也规范了充值和兑现操作，以避免洗钱和非法交易。

而FBI对于“丝绸之路”的查封行为并未引起比特币社区的过分担忧，为此叫好的也大有人在，这说明许多人都清楚：无论比特币是多么伟大的创新，拥有基本的法律和道德底线都是必须的。同时，比特币社区对于创新也一直秉持非常积极的态度，许多创意公司获得筹资的火爆程度是法币世界所无法想象的。自律、宽容、互信和民主必将更加充分地凸显比特币的价值，而如前所述，只要有价值的东西，就很难被封禁。

总之，在政府是否会封禁比特币这件事情上，我们没有必要杞人忧天。

06 辨是非

挖矿有意义吗

“挖矿”这个名词其实源于中本聪所谓的“计算散列值并对算出最终结果的人给予比特币奖励，该行为类似于挖掘黄金”的比喻。这个形象的比喻便于人们理解整个比特币系统的货币产生过程。但同时，这个比喻也产生了一些误解，使很多人认为挖矿的关键动作在于“挖”，其目的是发行新的比特币并将其注入这个金融系统。其实，这是一个错误的观念。

对于比特币系统而言，“挖矿来获得比特币”只是一个相对次要的目的，更重要的目的是通过这些计算来确保比特币的正常交易并防止重复支付，简单来说就是防止有人作弊。挖矿的关键动作不是挖而是维护，产出比特币只是一个副产品而已，仅仅是为了奖励那些为维护比特币金融系统做出贡献的人。所以，矿工的比喻其实并不准确，更准确的描述应该是印钞厂的工人、

银行员工、银行大堂里的保安和每次跟着押钞车一起来的荷枪实弹的押运武装人员。

所以，挖矿的意义并不是白白消耗电力和磨损硬件来做无意义的计算以获得比特币，而是通过大量计算防止作弊，维护整个比特币系统的安全。

中本聪对此也有一个侧面的说明，即早期的矿工收入来源于新增的比特币，而到了2140年，所有的比特币都挖掘出来后，矿工的收入则来源于交易的手续费。也就是说，矿工前后的收入方式是有变化的，这也就证明了挖或者说发行比特币不是一个永恒的行为，真正永恒的行为是维护。当然，中本聪的这个说法也是有偏差的，因为现在比特币用户传输过大或过小金额的比特币时，系统是要抽取手续费的，即矿工目前的收入已经是两种方式并存了，只是后者所占的比例将会越来越大，最终达到100%。

因为比特币的发行量是每4年减半，大概11年后，近94%的比特币将被开采出来。所以在这11年里，你仍然可以暂时将矿工视为矿工或者印钞厂的工人，但2024年之后，这个观念就必须转变了。

比特币是合理的金融系统吗

所谓的合理，就是维护该系统运转的成本是否划算，即手续费是否合理。比如，一个金融系统整体货币的流通量是100，而该系统内货币流通的手续费是10%，周转10次后，系统内的钱就全部被中间机构收走了，这显然不合理。然而，这并不是说手续费越低越好。道理很简单：一个镖局押10

万两黄金的镖，但因押镖收费极低，镖师只能雇用两个镖师，这趟镖的安全性将大打折扣。同样，你到银行存款，大概也不会在一家看起来破破烂烂的银行开户吧。

所以，一个合理的金融系统应该收取一定的费用，但这笔费用如果太高会不利于资金流转，若太低则不安全。那么，究竟多少才算合理呢？在现实经济中，银行业是维护现有货币系统正常运行的主体，矿工群体也可以认为是比特币系统的维护者。我们可以与银行业做个比较。2012 年，中国银行业净利润为 1 万亿元，总收入应该有 4~5 万亿元，M2（反映货币供应量的一种指标）则为 100 万亿，相当于 4%-5%的年运营成本。4%~5%的比例看起来很高，但这是年运营成本，如果在这一年里资金流转了 10 次，那么平均每次只需要 0.4%~0.5%，这其实和我们的汇款手续费差不多。

再来看看比特币系统。2013 年 5 月，粗略估算当天全网算力为 90 000G（因为全网算力和矿机价格一直在大幅变动，所以难以精确），网上 1G 计算力设备大概需要 700 美元，即全网设备价值为 6 300 万美元左右。

6 300 万美元的设备按两年折旧，每年损耗 3 150 万美元，算上电费和利润，矿工群体的总收入大致是 5 000 万美元，这即是比特币全网的运行成本。现在的比特币系统内共有 1 000 万个比特币，价格大致为 100 美元/个，共计 10 亿美元的总市值。计算一下便可知全网年运行成本相当于市值的 5%，和我国的银行系统差不多。

从上述分析中我们还可以推出一个比较违反直觉的结论：比特币世界要

想安全，就要尽快扩大规模，又因其新增货币量每 4 年就会减半，所以要扩大规模就只能把价格推高，即其币值越高，系统越安全。

市值越高，就有越多的矿工或者硬件设备来维护该系统。如果最终比特币形成一个 1 000 亿美元的金融系统，那么就会有成本为总量 5%，即有约 60 亿美元的硬件设备来保持其运转，要与这样的设备总量抗衡并发动 51% 攻击，难度就大大增加了。这和我们的直觉恰好相反，我们总觉得比特币币值太高会不稳定，实际上这样的思维是错误的，或者精确地说，短期内是对的，长期则恰好相反；对投机者是危险的，对投资者而言却是利好因素。

另外，现在对于 51% 攻击，大家普遍比较在意全网算力，但真正需要关注的是全网挖矿设备的总价格，因为无论全网算力有多高，如果一台超强的矿机只需很低的价格就能买到的话，想要实施 51% 攻击的人也可以廉价获得大量算力。从这点来看，唯一的解决方法就是使比特币的总市值尽快增加到足够大的规模。

比特币有价值吗

这个问题大概是目前争议最大的问题，黄金派、信用派和比特派各执一词，不相上下。黄金派的观点是，货币就应该是商品货币，没有价值支撑的货币都不是好货币。信用派的观点是，货币只要有政府强权来支撑并强制使用就可以，它是用国家信用做担保的。比特派的观点是，比特币几乎符合货币理论里对货币的所有定义，同时还优于黄金和信用货币。

所以，在贴吧、论坛和QQ群里常能看到三家互相批驳、互不相让的情形。比特派跟黄金派谈信任的时候，黄金派称信任再强也敌不过由国家军队的飞机大炮支撑起来的国家信用；跟信用派谈价值的时候，信用派称那些纯粹是无意义的数学计算只浪费电而已，再有价值也比不上黄金5 000年沉淀下来的价值。

既然如此，那么使比特币良好运行的内在机制又是什么呢？那就是：

1. P2P分布式结构使其无比顽强，除非互联网被关，否则它会一直存在；

2. 数学算法设定的发行上限使其天然具有保值功能；

3. 写入算法里的天然防伪功能；

4. 基于互联网的支付往往匿名、自由、安全；

5. 造币成本为零且无磨损；

6. 可无限分割。

比特币合理的内在机制使其无需外力也可运行。甚至更进一步，良好的系统与参与者的道德水平、精神面貌关系不大，这是由其内在机制决定的。实际上，比特币系统是如此强大、独立、自信，根本不需要信任、理解甚至热爱这些温情的玩意儿来粉饰自己。

回顾历史，之前无数信用货币都因其所依靠的政权的垮台而灰飞烟灭。而作为非信用货币，黄金在发展之初也曾遭受过质疑和拒绝，在灾世还遭受过唾弃，甚至在几十年前还曾被法律禁止过，可最终它历经数千年而屹立不

倒。良好的货币系统是有其顽强的内在生命力的，它不会随人的意志而转移。所以，不要去看这个货币背后的支撑力量有多强大，而应该关注这个货币自身是否强大。

比特币价格大起大落好吗

在分析之前，用两个小故事作为理论依据：一个叫刻舟求剑，一个叫小马过河。故事大家肯定都听过，但不知有多少人真正思考过。刻舟求剑讲的是用静止的眼光看待发展的事物，看不到客观环境和条件的变化；小马过河是说对自己缺乏正确的认知。

再说回比特币。优质的货币不应该大起大落，这句话本身并没有错，只是缺了一个定语——“成熟的”。一个应用广泛的货币当然不应该大起大落，但问题是，现在的比特币成熟吗？即便不考虑比特币现在所处的阶段，就套用货币最终阶段的表现——不大起大落，这种静止的观点不仅是对比特币的苛求，而且否定了事物的发展规律。

其实反问一句就能看出问题：如果现在比特币不大起大落了，你就会拿它当货币交易吗？你会在菜市场跟小贩一人抱一台笔记本或者手机用比特币做交易吗？显然不会，用钞票多方便！由此可以看出，比特币现在明显还处于很原始的阶段，缺乏相应的金融服务，缺乏足够多的商家支持，缺乏足够多的用户。最糟糕的是，这还是个鸡生蛋、蛋生鸡的关系，必须要有更多商家支持才有更多人使用，但商家也只有更多人使用了才会选择支持，这就成

了一个循环等待的过程。

所以，指望比特币现在就成为主流货币并起到普遍交换的作用是不现实的。现实情况是很多人都在做波段赚差价，或者被人赚差价。但也就是这些投机者把比特币的总市值从零推到了10亿美元。因此，对于比特币来说，务实的态度是承认投机者的积极作用，并且争取吸引更多投机者。

从这个角度来看，比特币现阶段的大幅波动并非全然是坏事。大量比特币交易者就是从投机开始，慢慢的就接受了它、承认了它，甚至习惯了它。当交易者越来越多，比特币的总市值越来越大，相应的金融衍生机构逐步增多，其使用愈加便利，更多的商家开始考虑接受并支持它，基于比特币的生态系统也随之逐渐繁荣，最终，我们就有可能将其作为货币使用。这样的发展路径不需要使用者有多么高尚的理想或者自觉性，对财富的追求和恐惧反而会帮助比特币向成熟之路迈进。

另外，我们之所以认为货币，如美元是稳定的，前提在于这个世界上有千千万万的商品和服务都是以美元计价的。要想在短期内使美元剧烈波动，就必须让所有这些商品和服务的标价也同时剧烈波动。美元不是自己在战斗，要想使美元波动，便要对抗整个商品和服务体系。与此类似，要让比特币币值稳定，就需要尽量多地让其与现实世界的商品和服务挂钩，即用比特币给商品和服务标价。挂钩的商品和服务越多，比特币越稳定。

所以，比特币的波动问题根本就不是什么问题，它唯一需要的就是时间，慢慢的让越来越多的商品和服务以比特币标价，它就会越来越稳定。

手续费、块链大小和转账速度

随着币值的升高，比特币的转账手续费会越来越贵；如果手续费率是固定比例，那随着使用人数的增多，块链体积就会激增；而且，转账速度因为算法限制，有时候确实比现有金融系统慢很多。

很多了解比特币技术的人对上述问题比较担心，并因此认为比特币最终难成大器。事实上，这并不难解决，只要我们允许中心化的比特币银行出现，即可实现瞬间转账和内部交易，同时还不占用区块链。

那么，这是否和比特币的去中心化理念相矛盾？比特币的去中心化主要体现在两个方面，一是运行基础去中心化，它是由无数平等的网点组成的P2P网络，没有中心节点；二是货币发行去中心化，没有一个央行来控制发钞。中心化的银行不违反后者，但会影响前者，所以从某种程度上讲确实存在一定矛盾，但这种矛盾可以带来诸多好处，可以说是自由与代价之间的折中选择。

当出现中心化银行时，愿意使用比特币系统的人还是可以继续使用比特币系统，只需交纳手续费和忍受较慢的转账速度便可实现匿名的全球转账；希望快速转账而且不愿意安装和使用客户端的用户可以选择比特币银行。其实，这样也同时实现了比特币全网良好的资源配置，随着手续费的提高，让用户根据自己的需求自行选择。换句话说，自由和匿名是有价的，这反过来也意味着，只要你愿意花钱，就可以买到自由和匿名，而这在以前是难以做到的。

比特币是通缩货币吗

虚拟货币常被人诟病的一个方面是：机构超发虚拟货币怎么办？但和其他虚拟货币不一样，总量不超过 2 100 万个的比特币面临的一个问题是：不够了怎么办？这个“不够了”其实包括两个问题：一是流通所需的数量不够，二是通货紧缩。

关于流通所需的数量不够的问题实际上是不存在的。若大家都习惯用纸币交易而不是银行转账，那对纸币的需求量必定会增加。但对于电子货币不存在这个问题。它就是一串数字的转移，不涉及持有的“货币实体形式”。

我们也不要被 2 100 万个的“个”字误导了。比特币不是实体货币，不可切割拆分来使用。2 100 万张 1 元货币，没法解决支付 0.5 元，或者 2 101 万人需要持有的问题。但是电子货币不需要物理拆分，只需要发明更小的单位或者借助小数点就行了。

对于通货紧缩的问题，虽然比特币可能存在很多缺点，但是通货紧缩特性绝对不是其中之一。瑞典海盗党派主席理查德 · 法尔克维奇认为，我们对通货膨胀已经深有感触：货币越来越多，央行超发货币获得铸币税，我们手里的货币却在贬值，但是我们对通货紧缩似乎并不熟悉。其中最常见的一套说辞是这样的：如果商品会在将来变得更便宜，那么就没有人愿意在当前使用货币进行消费；而当未来的物价下跌时，由于物价还会变得更加便宜，因此人们还是不消费。所有人都将无限期地节制购买欲望，以等待物价下跌。

但事实或许不是这样的。反过来想，如果我们因为某种商品明天就要涨价，我们就迫不及待地将手中的钱花出去。那么，我们就会立刻购买所有我们能够购买的商品，这看起来是不是很荒谬？

虽然经济体从整体看来没有经历过通货紧缩，但是在某些行业，已经经历了几十年的通货紧缩。假想一下，如果某种商品在 3 个月之后将比现在便宜得多；而再 3 个月之后，价格还会继续下降。那么你是不是就会一直等下去呢？

电子产品行业从 20 世纪 70 年代开始，就一直处于通货紧缩状态。大部分电子产品在几个月后肯定会变得更加便宜；如果你愿意等上两年，甚至可能会变得一钱不值。这就是通货紧缩——价格逐步下跌，而你的钱变得更加值钱。

此外，稳定的通货紧缩只会发生在无弹性货币体系中，比如黄金、比特币，通货紧缩非但不会破坏经济，反而会促进经济发展：如果货币体系回归诚实货币，不具备金融市场投资知识的人们，以及没有能力聘请投资顾问的人们，只需要简单地持有诚实货币，即可实现一定程度的投资收益。因为在那种货币体系中，随着社会财富不断积累，币值会稳定反应物价上涨幅度，不存在货币贬值的问题。当然基于个人投资能力高低，优秀的企业家和投资者将获得更合理的回报。而这样的事情是不可能发生在纸币系统中的，持续的通货膨胀和失控的货币体系将慢慢夺去人们积累的财富。

如何正确看待比特币的发展

比特币仅仅用了4年多就拥有了10亿美元的市值，同时还成立了交易平台、股票市场等相关金融机构，那么未来比特币还会有哪些发展呢？我们不妨用回归历史的方式预测未来，就如同2D（二维）人通过投影的方式分析3D（三维）物体那样去分析4D（四维）世界的一些几何性质。

人类社会的发展趋势

1961年，加加林代表人类第一次进入太空；1969年，阿波罗11号首先实现了载人登月。20世纪50年代出生的孩子们在那个时代肯定会浮想联翩，相信自己在不久的将来一定有机会进入太空。哪怕是20~30年后出生的我们也一样，看着七八十年代写成的科幻小说，憧憬着20~30年后发达的人类社会，相信人类会大规模进驻太空站、移民月球或者漫游星际。

而出人意料的是，这几十年我们真正发展起来的是微处理器、软件和互联网。这给了我们一个非常明确的人类发展方向的启示，即人类改变了几千年来一直遵循的更高、更强或者更远的进化方向，而选择了更快、更智能。从现阶段的发展看，人类越来越倚重互联网这个虚拟世界，它把人类像大脑细胞一样组织起来，形成了更高级的智能。可以说，人类正在大规模地由现实世界向虚拟世界转移，我也相信，不管我们是自愿的还是相互胁迫着，人类社会的未来将走向《黑客帝国》而不是《星球大战》。

我们是从向外界索取物质变为向内在深入挖掘自身潜力的方向发展。其

实宅男腐女的现象并非我们所看到的那么简单，为什么以前的时代没有这么多，我觉得这代表着虚拟世界在大量地替代原来实体世界能够实现的功能，所以宅在家里依然能够过上正常的生活。

改变未来的经济形态

如果你能接受人类社会将越来越倚重虚拟世界的观点，那么在全面进入之前，我们必须首先思考一个问题：我们的虚拟世界足够安全吗？互联网曾因其分布式结构赋予的安全性和可靠性而受人称赞，但是互联网上的一些重要资源——例如DNS（域名解析系统）根服务器和云服务器——分布过于集中，展现出中心化的弊端。最近的棱镜计划则显示了当前互联网对于隐私、自由和安全的保障何其脆弱。

比特币的运作方式告诉我们，所有的交易记录可以被分散化存储，那么DNS是否同样可以呢？如果真的可以，从此互联网世界将彻底打通，任何网站都无法被彻底屏蔽。如果服务器空间变成一种P2P去中心化的全球云，所有的网站内容都可以放在上面而不用担心网站会在一夜之间被关闭。

这看起来似乎有些不太现实，可实际上这些服务大部分早就实现了，比如域名系统在Tor里已经实现，而且Tor还采取P2P互联的方式让各个客户端之间相互帮忙传递流量，从而使得网络无法被封锁。电驴其实就是一个巨大的网络硬盘，它早期还要依赖服务器，后期有了KAD（一种分散式的P2P通信协议）网络后差不多就是一个去中心化的全球下载站； BitTorrent之后的

很多新P2P下载技术，比如磁链，也开始慢慢向去中心化的方向发展。既然早就有了，为什么我们还要说比特币系统给了我们很大的启发呢？

说到底，上述的Tor和电驴之类的P2P服务都有一个致命的缺陷，即它们都是依赖谦谦君子和道德楷模的系统，对使用者的道德和自觉性要求极高，内建的激励机制并不强，所以大部分人都是用的时候开启客户端，用完就走人，特别是BitTorrent下载，每次充当“种子”的人都要呼吁希望大家留种。但是反观比特币的矿工，根本没有人要求他们购置硬件、消耗电力甚至忍受巨大的散热风扇的噪音，可他们依然踊跃地去做这些事情，就是因为有巨大的物质刺激。

如果把比特币的这种思路嫁接到自己身上，上述这些服务将会获得翻天覆地的变化：有人会长期挂Tor，因为可以赚Tor币；有人会专门买硬盘阵列来当“种子”或者做电驴共享，因为可以赚驴币（电驴官方奖励用产的网络积分）等。当然，最后他们也许会发现，直接使用比特币的技术框架来实现这些功能最简单，流通性也最强。

再推而广之，这种引入激励机制的去中心化P2P服务将会横扫一切不需要人力参与的第三方服务行业。保险业是需要人为鉴定的，所以无法用算法和互联网取代，但对于支付宝这类第三方中介，使用一个简单的纳什均衡就可以解决，并不需要真正的第三个人来充当中介，去中心化交易平台NashX就在做这样的尝试，如果成功就可以解放大量的人力，极大地降低社会成本。

所以，比特币思想及其系统本身对未来的影响之深远有可能是今天的我们无法想象的。它甚至有可能从货币领域影响经济领域，最终改变整个人类的意识形态和政治格局。

比尔 · 盖茨说过，人类总是高估 3 年内的变化，却低估 10 年内的变化。所以已经走过 4 年的比特币将在未来 6 年开始对全球产生真正的第一阶段的影响，其标志就是某个产业或者国家正式宣布全面支持它。而我们唯一需要的就是再多一些耐心。

07 虚拟货币体系中的比特币

把比特币仅仅看作一种货币，而不是一种革命性的思想或者一整套交易生态和架构，那显然是小看比特币了。即使把它的影响限定在更广的金融领域，也未必是合适和恰如其分的。但是就目前来讲，比特币的货币属性还是被无限放大，虽然人们很少思考货币本质的问题。

在公众的常规理解中，比特币既非法币，也非具备物理形态的稀有贵金属，更没有得到社会的普遍认可和信任（至少暂时如此）。其流通的范围和影响力均有限，通常只能被归于虚拟货币的一种。如果全球货币系统是广袤的大地，那么充满神奇色彩的比特币仅仅是一粒细小的流沙，虚拟货币大概是流沙集。但是，这个流沙集的潜在核心是否是比特币尚待观察，虽然许多人对此充满渴望。

这些命题很自然地就会引出一些疑问：虚拟货币和我们常说的货币或者

法币有什么区别？其产生、流通、发展的基本逻辑是什么？比特币与其他虚拟货币有什么区别？它有没有长久生命力？

货币简史

从实物货币到符号货币

货币并非是天然产生的，而是源于物品交换的需要。原始社会时，人类生活状态为自给自足，偶尔零星的交易通过直接的物物交换即可达成。随着历史的演进，人类社会产生分工，物物交换的弊端日益明显，必须存在双重巧合才能达成交易：交换双方都需要对方的物品，且待交换的物品价值正好大致相等。为了解决这一问题，人们逐渐采用某种具体的物品作为特殊商品，以其为中介，先把自己的物品交换成一定数量的特殊商品，然后使用该特殊商品购买自己想要的物品。

这种特殊商品就是货币。由于特定区域的不同生产条件和生活方式，早期货币形式多种多样，如我国夏商时代的海贝、古印度的牲畜、古巴比伦人的大麦、美洲的可可豆和烟草等。伴随经济的进一步发展，交换的范围日益扩大，对货币的要求越来越高，包括：便于携带、储存、计量，不易磨损，价值稳定等。金属（如金、银、铜、铁等）在这些方面存在较大的优势，导致形形色色的货币类型都逐渐向金属货币集中，取代了自然货币和其他材质的货币。

金属货币在数千年的历史中，一直伴随着两种演变：由贱金属（如铜、

铁）向贵金属（如金、银）演变，由称量货币向铸币演变。前者使得货币的材质更加集中，后者使得货币的发行成为一种权力。这两种演变在西方国家表现得尤为明显。在公元前后的古罗马帝国，恺撒实施了金本位，奥古斯都则把金币与银币的铸造规定为皇帝特权。

但金属货币有重量过重、磨损较高、携带不便的缺点，逐渐也不适合频繁的大范围交易环境，作为金属货币象征符号的纸币就此产生。我国南宋时期的交子、欧洲 17 世纪的银行券都是早期的纸币。早期欧洲纸币和我国的银票相当于金属货币持有凭证，以金属货币为基础，与金属货币可以自由兑换，二者可同时流通。

19 世纪末，西方经济出现了速度空前的膨胀与发展，纸币逐渐成为主要的流通货币，但仍然以贵重金属储备作为发行保证，历经银本位、复本位和金本位的演变。约同一时期，工业化国家先后禁止商业银行发行银行券，并把权力集中于中央银行。当时与银行券同时流通的还有一种由国家发行并强制使用的纸质货币。有的国家所称的“纸币”（paper currency，paper money）专指这种钞票。

1929~1933 年的世界经济危机后，任何形态的金本位都不复存在，代替它们的是不兑换银行券制度。在国际货币体系中，为应对金本位消失后的货币兑换比率问题，曾短暂实行过金兑换本位制。“二战”末期，美国占据世界经济中心地位，44 个国家形成了以美元为中心的布雷顿森林体系，确定了美元的含金量，其他各国货币按其含金量与美元定出比价。

1971 年 8 月 15 日，美国宣布停止向各国政府及其中央银行按照官价兑换黄金，这实际上意味着绝大多数国家的货币与黄金切断了最后一丝联系，全面进入纸币本位制时代。国家不规定纸币的含金量，也不允许纸币与金（银）兑换，纸币作为主币流通，具有无限法偿能力。中央银行通过信贷程序发行纸币，纸币成为信用货币。各国一般根据经济发展的需要决定纸币发行量，并对其实行严格的管理，称为“有管理的通货制度”。

简要回顾货币历史，可以发现，货币的发展表现出 3 个典型特征：货币材质去实体化、货币价值虚拟化和货币职能符号化。

货币材质去实体化

从各种各样的天然货币（如牲畜、粮食、贝壳等），到金属货币（金、银、铜、铁等），再到纸币，货币的材质一直在发生变化。这种变化与经济规模的扩大、交换范围的扩大、交换频率的大幅度提高相适应，便于货币货币职能的发挥。

1952 年，美国加利福尼亚州富兰克林银行率先发行银行信用卡，标志着一种新型商品交换中介的出现。美洲银行从 1958 年开始发行美洲银行信用卡。1973 年，罗兰德 · 莫诺发明了IC卡，作为电子货币的存储介质。1982 年，美国组建了电子资金传输系统，随后英国、德国也相继研发了类似系统。以银行卡为代表的电子货币迅速流行，占据当今货币形式的主流。

电子货币使得货币彻底去实体化了，虽然我们仍然会使用卡片作为电子

货币的载体，但是卡片本身并不是货币，真正的货币是卡片里存储的数字。如同早期纸币对应于金库中相应价值的黄金，早期电子货币也对应于银行中相应数额的纸币。但是随着各国货币的发行转向电子化，电子货币也日益与纸币脱离，成为纯粹数字形态的货币。

据媒体报道，瑞典有可能成为全球第一个无现金的国家。2012 年 3 月，国际清算银行的报告显示，纸币和硬币只占瑞典货币量的 3%，与之相比，纸币和硬币在欧元区国家占 9%，在美国占 7%。在瑞典大多数城市，公交车不接受现金，车票钱必须预付或用手机短信支付。连一些小公司都只接受银行卡，很多银行的分支机构已经完全停止处理现金业务，通过电子交易业务进行支付和转账。

货币材质的去实体化有利于货币的携带、储存、使用和流通，尤其是随着无卡支付的盛行，货币甚至不再需要银行卡承载，在网上即可使用支付、转账等大部分的货币流通功能。较之传统的实物材质货币，电子货币具有如下优点：

便于携带和使用，无法损毁（卡坏了不代表卡里的资金不在了）；

中转快，便于流通，省却了纸币印刷、清点、搬送、运输、回收的费用；

易于防伪和管理；

打破地域限制，只要商家愿意接受，消费者可以较易获得和使用多国货币。

由于发行成本低廉，中央银行和商业银行之外的非金融机构都拥有了发行货币的可能性，例如机构货币、社区货币等，虽然这些货币的流通范围有限，但是在特定领域内，它们确实可以承担货币职能。

这些便利大大降低了货币的发行与使用成本，为社会带来额外收益。例如瑞典的银行抢劫案已从2008年的110起骤降至2011年的16起，这是该国有记录的30年内最低。但与此同时，电子货币存在严重的网络安全隐患。根据瑞典全国预防犯罪委员会的报告，包括隐瞒收入在内的网络欺诈案已从2000年的3 304起上升到2011年的近2万起。

货币价值虚拟化

与货币材质去实体化相伴的是货币价值的虚拟化。天然货币，例如牲畜、粮食，具有切实的实用价值，可以役使、充饥。早期金属货币使用的铜和铁可以打造农具、器械、兵器，同样具有较高的实用价值。当货币的材质由贱金属过渡到贵金属，货币本身的实用价值已经大大降低——金、银虽然也可以用来铸造器物，但人们看重的只是其观赏价值（工业价值则是很久以后的事情）。

纸币本位的出现，意味着货币本身价值基本消失。纸张即使再昂贵，与其票面价值相比也可以忽略不计。而货币的电子化则导致其实用价值的彻底消失。从铸币和纸币的国家化发行开始，货币本身价值的缺失由国家信用填充。大部分国家增发基础货币时，均有政府资产（或债务的收益权）作为抵

押，基础货币相当于政府向全国国民的借债，但至于借债是否能被偿还，乃至政府资产是否有价值，只取决于人们对政府的信心和政府自身的信用。

这就是当前绝大部分货币被称为“信用货币”的由来。基础货币发行之后，由银行借贷所产生的货币乘数效应，把政府的债务逐级放大。政府和金融系统是否真有能力清偿如此庞大的债务，无法得到实际验证。如果人们可以自由评估国家信用，自发选择是否接受由此国家信用支撑的货币，这一体系并无太大问题。但是，各国政府普遍规定了货币只能由国家发行，并强制法币的流通，导致人们并无自由选择的权力。此时政府信用的好坏乃至有无并不重要，货币变成供需决定的产物，成为经济调节工具。

货币价值的虚拟化源于材质的虚拟化，在货币材质本身失去任何实用价值，并与货币生产的实际成本脱钩之后，货币的价值已经无从度量。这种变化一方面意味着拥有货币发行权力的机构获得了凭空创造财富的能力，同时也意味着货币的价值支撑未必要与实物相联系。

货币职能符号化

货币的职能包括价值尺度、流通手段、储藏手段和支付手段，其中最基本的职能是价值尺度和流通手段。货币在执行价值尺度的职能时，并不需要有现实的货币，只需要观念上的货币。在实物货币时代，这种观念上的货币以足值的实物为基础，在商品价值量一定和供求关系一定的条件下，商品价值的大小取决于充当足值货币的实物的价值大小。货币作为流通手段则必须

是现实的货币，但它可以是不足值的。

在非实物货币（包括纸币和电子货币）环境下，货币的所有职能都符号化了，货币成为一个记账单位。例如，执行价值尺度职能时，货币只意味着某种大致的、难以量化的购买力，一种商品的价格是否合理，取决于两个因素：与其他商品相比，该商品的价格是否合理；购买者主观上认为该价格对于满足其需求是否合理。实际上这意味着货币丧失了直接的价值尺度职能，作为标尺，它存在较大的弹性和主观性。

执行流通职能的货币已经无法区分清楚现实与观念，它只是一串数字（符号），资金的变化只表现为数额的增减。只是这一数额的增减必须发生在某个物理系统之中，例如银行的账本或数据库中的记录。

货币职能的符号化是货币材质去实体化和货币价值虚拟化的必然结果。这种结果导致货币的面目日益模糊，它成为货币发行机构免费生产的商品。该商品无内在价值，其价值更多取决于供求关系，即如果货币发行机构生产的商品数量过多，其价格便下跌，产生通货膨胀；若生产的数量过少，其价格上升，产生通货紧缩。由于货币的生产成本极其低廉，发行机构的产量并未受到真正的制约，仅由发行政策决定。

货币职能符号化直接导致虚拟经济的兴起。例如，评估科技公司的价值，大多既不以其固定资产、人力资产作为估价依据，亦不以其盈利能力作为估价依据，而是通过某种曲折的手段——例如该公司的产品有多少用户、未来每个用户可能为公司带来多少营收——来估值。这些价值当前不存在，

未来也不一定存在，但是估值一旦完成，该公司便具备了相应的票面价值，投资蜂拥而来，票面价值变成银行账户里的现金。此时货币的数目增加了，但是现实世界里的实际价值并没有任何增加。如果该公司破产，与此相关的超发货币并不会消失，这在实物货币的时代难以想象。

货币职能符号化的利弊问题牵涉过广，难以尽述。它带来的另外一个结果是：我们实际上需要的并不是货币，而是一个总账本。如同质量的单位是千克，长度的单位是米，我们根本不需要千克和米的实物，我们需要的是国际千克原器、国际米原器这些能够衡量质量和长度的标准实物。与此相反，货币已经没有实物，也就失去了作为标准的含义，它可以仅作为获得共识的记账单位存在。

如此一来，个人财富的变化将表现为总账本下对应个人账目的变化，货币流通过程表现为总账本下对应买卖双方账目的同时变化。在此假设下，如果我们允许不同人群使用不同的记账单位，就意味着他们在使用不同的货币。在某种程度上这相当于回到了原始时代，人人都可以自由选择商品交换的媒介。

虚拟货币的产生

传统虚拟货币的形成和虚拟社区的发展息息相关，而虚拟社区的发展无疑是互联网的普及和人类需求相匹配的结果。虚拟社区包括社交网络、商品交易网络、在线游戏网络等多种形式。大家对此早已熟悉并且可能早就深陷其中了。社交网络包括人人网、QQ、微博、微信等，商品交易网络包括淘宝

网、当当网、亚马逊等，虚拟游戏社区包括《魔兽世界》、《梦幻西游》、《征途》等。此外，还有知识网络社区，比如新浪爱问、百度文库、维基百科等。诸如此类，不胜枚举。

当这些服务网络和货币联系起来的时候，你想到了什么，Q币、当当的购物积分、游戏点卡？甚至连人大经济论坛都需要虚拟货币。在某些情况下，这些虚拟社区通过创建并流通自己的数字货币来交换他们所需的商品和服务，从而为特定的虚拟社区提供一种交换媒介和记账单位。

当然，虚拟货币不仅仅在于创造一个新交换媒介和新记账单位，它的产生原因是多样化的。首先，它是商业模式的一部分，方便收取增值服务费用，同时也为虚拟社区的服务提供便利的小微密集支付服务，而不是把社区置于繁复的金融体系之下，它是灵活经营模式的必要部分。其次，它们往往可以为客户提供财务激励，以使用户继续参与其中，比如航空公司通过里程积分兑换提高客户黏性。最后，虚拟货币产生的沉淀资金（若非双向兑换流通）还可以为社区带来时间收益和残值收益。当然，最重要的支撑是这些虚拟货币的发行和分配是在虚拟社区的控制之下的。

而不管从逻辑还是实践上讲，比特币及其追随者都不直接与特定的虚拟社区相关，也不是为了购买虚拟社区的服务而产生，或者说，不需要特定虚拟社区的服务为其价值背书：它依赖的是互联网点对点产生的协议信任，并在此基础上提供包括支付、保护私人财产在内的庞大价值。

虽然比特币的初衷未必是获得货币地位——甚至可能没想过成为货币，

但其运行结果导致自己成为法币的直接竞争者。它是在本源上不限制自身流通范围，也不绑定特定的服务。正是因为这样，它必定与去中心化、总量恒定联系在一起，虽然后者是一个既定事实而非推论。否则，要是存在一个不受控制的发行方，又如何获得信任呢？而去中心化和总量恒定则意味着不存在严格的发行和控制方。[①]

这种去中心化和不嫁接某项服务的设计使其不存在受益的发行方。虽然最初开始挖矿的矿工有更多机会获得比特币，但是那与他们为建立和维护比特币系统做出的贡献相匹配。比特币的产生基于一种理想化的愿景——建立高效、便捷、低成本、点对点的现金支付系统。其创始人中本聪虽然受到多方关注，但事实上，他甚至无法对比特币体系施加任何影响。中本聪也从未用货币来形容比特币。就比特币的发行来讲，仅仅是这样一个美好的愿景，而不是一种商业模式。基于比特币的商业模式都是后来延伸出来的，与比特币的产生并无直接关系。

虚拟货币的分类

先援引一下欧洲央行对虚拟货币的定义和总结：一种不受监管的数字货币，通常由其开发者发行和控制，为特定虚拟社区的成员使用和接受。这些虚拟货币既和货币类似，又和它们专用的零售支付系统伴随、相关。

① 比特币也存在全网51%攻击的可能，严格来讲并不是“完全不受控制”，但与传统的控制概念完全不一样。

“货币”这个词太扎眼了，而且可能与各国法律相悖，所以有时候这些虚拟社区的经营者习惯把它称为“储值账户”，就好比健身卡、饭卡。这里面的界限比较模糊，虽然未必符合货币的所有定义，却承担了某些类似货币的职能，尤其是那些流通范围不局限在特定虚拟社区，且能和法币实现双方兑换的虚拟货币。这里暂时把它们统称为虚拟货币。

显然，欧洲央行因为对比特币的了解不够深入，才会把虚拟货币定义为“由其开发者……控制”，“专用于某个零售支付系统（倒也并非某个虚拟社区）”，同时却把比特币归为虚拟货币，因此我们需要对欧洲央行的虚拟货币定义做一些延伸。

这种延伸事实上是要为传统虚拟货币和新型虚拟货币做一个界定。假如把中心化的、流通领域限于特定（支付）范围的虚拟货币称为传统虚拟货币。新型虚拟货币则可以用这么几个核心概念来定义：去中心化，不受其开发者或者其他人完全控制，总量恒定；流通领域不受限制，只取决于使用者的意愿。

事实上，还没有人对虚拟货币做如此划分。或许有人会说：你干脆把虚拟货币分为比特币和非比特币好了。我的回答是：不对，应该是比特币及其追随者（例如莱特币等）和其他虚拟货币。毕竟在这种思想下，新型虚拟货币可以不止有比特币一种形式，虽然目前来看比特币是相对完美的一种。

对分类的界定与研究者的角度设定有关，没有定式。逻辑可以分为多个角度和标准分类，和其他研究一样，我们也只选其一。我们只是认为这样的分类方法更能揭示一些本质性的东西。

我们是按照虚拟货币的发行和职能进行分类的。常见的分类是什么？其实判定者心中已经有了法币的核心定位与标杆，他们是按照虚拟货币能否与法币产生兑换进行分类的。但是，这个兑换问题难道不应该从属于其发行和职能吗？在其他虚拟货币还在遮遮掩掩地宣称自己是“储值卡”的时候，比特币从一出生就把自己放到了与法币竞争的位置上。从货币这个角度讲，我认为这样的分类符合逻辑。当然，流通和兑换的问题也很重要，后文会详细论述。

此外，还要区分两个概念。一个是电子货币。电子货币的概念常被混用。假如说电子货币是基于电子形态的货币，只着眼于与物理形态的区分，那自然也就包括虚拟货币了。不过，本文要区分的是中央银行发行的电子形式的货币，也就是电子法币，是替代纸币流通的电子数字。比如我们存在银行的那些数字，还有中央银行账上更庞大的数字。这些数字是和虚拟货币完完全全不一样的。另一个是去中心化。去中心化并不是结果，而是一个反复不断的过程。这一过程不断摧毁已有的中心，并产生新的中心，在此过程中形成新协议和新标准，体现出更加公平、合理、普惠的契约精神。我们需要关注的是去中心化过程的稳定性以及每次变化的成本。

虚拟货币的流通

虚拟货币的发行一般被认为是由特定的虚拟社区和私营机构控制，直到比特币出现。正如前文所讲，传统虚拟货币与虚拟社区的服务息息相关，这也是它与新型虚拟货币最明显的本质区别之一。

至于流通，我们主要关注它与法币之间的关系。目前虚拟货币还是局限于某些领域和某些人群；一旦可以与法币自由兑换，那就实现了间接的大面积、多渠道流通。大部分虚拟货币在诞生之初与法币并无关联，严格意义上也不存在绝对不受控制的发行方，流通性很差。比如，一些在线游戏的积分和游戏币只有通过游戏升级才能获得和使用，而且只能用于购买游戏之内的服务。再比如航空公司的里程积分、大型商场的购物积分，诸如此类只能兑换本体系内的货物。在这个意义上，它们是完全封闭的，几乎不像货币，或者说是内部账本、内部货币。

不管是平台有意还是民间自发，这些虚拟货币逐渐开始有了单向流——用法币就可以购买，或者接受一些等值的交换。交换方案由虚拟社区根据市场实际接受能力拟定。但既然有了单向流，根据价值传导机制，只要对方接受该虚拟货币，很自然地就可以用其购买其他商品和服务了。

再接下来，它们就实现了双向流，可以用虚拟货币直接购买社会上的商品和服务，也不局限在虚拟社区里面，甚至可以与法币自由兑换。虚拟货币和真实货币（包含法币和相关一般等价物）的界限逐渐模糊。虚拟货币成为法币的竞争者。不过，囿于法律规范，平台本身可能并不承诺反向兑换，不从事货币双向经纪业务。在技术几乎不可禁止的情况下，自发的机构或者民间平台开始发挥作用。国内对于虚拟货币和人民币之间的双向兑换流通是有限制的，但是这种限制似乎也不受控制。腾讯公司表示其发行的虚拟货币Q币和人民币之间不会双向兑换，但这种兑换却自然形成了：在很多电商平台

和论坛上，都有销售和购买Q币的信息。

我们采用典型案例来做具体介绍。

魔兽世界金币是该角色扮演游戏中使用的虚拟货币。玩家有不同的选择（具有不同的订购费）来开立账户并开始游戏。魔兽世界金币作为交换手段在游戏中是必需的。例如，玩家为了得到更好的装备就必须使用金币。玩家在游戏中有一些机会来赚取金币。在现实世界中，购买和出售魔兽世界金币是被其开发方暴雪娱乐公司的条款严格禁止的。

Facebook Credits是Facebook于2009年推出的虚拟货币。其目的在于允许用户购买Facebook平台上所有应用程序中的虚拟物品。这种虚拟货币可以使用信用卡、Paypal账户或多种其他付款方式购买。使用美元以外的货币进行购买时需要根据当日汇率转换成美元，然后以1Facebook Crebits=0.1美元的汇率兑换为Facebook Credits。用户还能够通过特别促销活动获得额外的Facebook Credits。令人惊讶的是，2012年6月，该公司宣布即将“更新支付产品”，且自2012年7月开始，所有以Facebook Credits表示的价格和结余将被转换为当地货币金额。

林登币是在《第二人生》中发行的虚拟货币。《第二人生》创造了一个虚拟世界，用户可以在其中创建化身，即可定制数字角色。《第二人生》有自己的经济，用户可在其中互相购买或出售商品和服务。为了做到这一点，他们需要林登币。而林登币可以根据外汇交易市场的汇率用美元和其他货币购买。信用卡或Paypal账户是必要的。用户也可以出售自己多余的林登币以

换取美元。

而比特币完全不同。实现与法币的自由兑换是体现比特币影响力的重要表征。但从另一个方面讲，既然是法币的竞争者，比特币明显不是为兑换而来。其影响和潜在思维也与上述传统虚拟货币大相径庭。其理想中的流通是基于自身体系的，而非与法币的兑换通道。以能否实现法币兑换来区分比特币的性质也就不合适了。

如上文所说，比特币不是为了购买虚拟社区的商品和服务而产生的，它是狭义的货币，是法币的直接竞争者。其流通性和法币在理论上是一样的，甚至更广——法币只存在于某一个法律涵盖下的国家实体里，比特币通往世界上任何有互联网的地方，可以与法币直接双向兑换。假如比特币总量受到限制且得到充分信任，法币却被不断超发，两者的职能又是基本类似，为什么要把比特币兑换成法币呢？除非是法律强行禁止——但是事实上法律是没有办法禁止互联网的，也就没有办法禁止比特币。

虚拟货币与政策

传统虚拟货币主要是作为商业模式和微型支付工具存在的，其便利性促进了电子商务、网络社区以及其他虚拟网络的发展。虚拟社区和网络的发展又推动了传统虚拟货币功能的延伸，传统虚拟货币的职能也在不断丰富，很多已经被视作“准货币”。对传统虚拟货币来说，最常被讨论的话题就是应该怎样监管，而这些都是基于传统虚拟货币的风险的。

比如发行人信用的风险。第一，发行人是否都能提供对应的服务支撑？举个极端的例子吧，假如腾讯破产了，该怎么办？在外的Q币所对应的服务无法继续提供，只能在破产清算中得到有限的赔偿或者根本就得不到赔偿。法币会不会也无法得到兑现呢？会的，当国家破产。但是因为权力机器的存在，有作为超稳定现金流的税收保障，还可以以正当名义超发货币，征收铸币税，国家破产的可能性很小。第二，发行人超发虚拟货币的风险。这和央行超发货币引起法币贬值是一样的道理。此外，还有缺乏回兑机制和回兑信用保证等相关风险。对此，有人提出，央行应该首先成立资产清查小组，对各发行商进行不良资产清查，保证虚拟货币发行行为在其能力控制范围内，但是这是一项非常艰巨的任务。

再如冲击现有货币体系。当然，冲击货币体系并不一定是错误的，只要有利于社会整体效用和福利的提升就行。但如果这种冲击极大地影响了社会金融稳定，那就可能存在问题。当虚拟货币真正实现和法币挂钩和相互间的全流通后，虚拟货币也就完成了从虚拟到现实的跨越，成为真正的货币。目前，国内的金融体系尚难于适应多种货币和多种支付体系。虚拟货币也影响了现有商业银行的现金管理等服务，对中央银行统计观测M0（流通中现金）和M1（狭义货币供应量）产生影响，也会影响货币政策的有效性。

文化部、商务部发布的《关于加强网络游戏虚拟货币管理工作的通知》规定："网络游戏虚拟货币的使用范围仅限于兑换发行企业自身所提供的虚拟服务，不得用以支付、购买实物产品或兑换其他企业的任何产品和服务。"

这就严格限制了网络游戏中的虚拟货币的流通。

此外还有洗钱、网络安全等问题。不过，片面指责其洗钱和用于其他违法犯罪活动也是不太公平的。一直以来，由于比特币高度的匿名性，人们觉得它可能会成为一个合适的货币替代品来进行毒品交易和洗钱，以及相关的其他非法活动。然而，相同的问题在使用现金时也可能发生。现金也可用于毒品交易、洗钱、逃税等。问题不在于货币的形式，而在于使用者用它做什么。不过，如果使用数字货币本身会使调查和执法复杂化，特殊要求可能是必要的。

欧洲央行的虚拟货币报告站在央行的角度，从宏观层面对这些风险及相关结论做了总结，主要包括物价稳定的风险、金融体系稳定的风险、支付体系稳定的风险、缺少监管的风险和央行信誉风险。

报告主要内容有：

1.倘若虚拟货币创造保持在较低水平，就不会对价格稳定构成风险；

2.虚拟货币存在内在不稳定性，但并不会危及金融稳定。这是因为它们与实体经济的联系还有限，而且交易量较少，缺乏用户的广泛认可；

3.尽管参与虚拟货币方案暴露了用户的信用、流动性、经营和法律风险，但其目前仍不受任何公共机构的严密监管和监督；

4.考虑到这些方案面临的法律上的不确定性，它们可能被诈骗犯和洗钱者用来实施非法活动，这可能对公共当局是一个挑战；

5.假设虚拟货币的使用大幅增长，而公众认为这些事件部分是由央行工作不力造成的，新闻媒体的报道可能会给央行的信誉带来负面影响；

6.支付体系产生了对虚拟货币发展研究的需要和初步评估的条款，而虚拟货币方案与支付体系具有一些共同的特征，相关内容涉及央行的责任。

虚拟货币是一种在实践中演变出来的体系。从概念的角度讲，它与真实货币及支付体系相比，呈现出一种实质性的变化。第一，传统的参与者如金融机构、结算公司和央行与这些方案无关。第二，在互联网的访问和使用获得巨大增长和技术创新的背景下，它们更容易衍生化。而且它们往往并不固定于一个特定的国家或货币区，这使得制定法律、监管和执法变得复杂。就金融创新和为消费者提供额外的支付选择而言，虚拟货币实践有积极的一面，但很显然它们也有风险。

欧洲央行同样提出，虚拟货币的增长将会继续，原因如下：互联网访问量、使用量的增长和虚拟社区用户不断增长；电子商务的增长尤其是数字商品对虚拟货币方案来说是一个理想的平台；和其他电子支付手段相比，通过虚拟货币支付可获得较高的保密性；和传统的支付体系相比，交易成本较低；清算结算更直接、快捷，这是虚拟社区更为渴望和需要的。

欧洲央行的总体结论则中规中矩：鉴于目前的风险评估更依赖于规模相对较小的虚拟货币，而虚拟货币还将继续增加和成熟，这意味着需要定期检查发展以重新评估风险。

但有一个问题是，欧洲央行的研究是从央行的角度出发的，其本身已经隐含了央行需要扮演什么角色的命题，而去中心化思想的立论却是政府及央行不需要做什么。角度的不一致使之没有办法谈及货币领域自下而上的去中心化的契约重构问题。也就是说，它们其实在一定程度上低估了比特币及其追随者。

比特币的独特价值

在竞争中发现最好的货币

与虚拟货币紧密关联的一个话题就是竞争性生产货币。哈耶克晚年转向了货币领域的研究，著有《货币的非国家化》。他在书中提出：假如在其他领域已经证明，竞争产生效率和好产品，那么在货币生产和流通领域是否也可以竞争呢？具体来说，废除中央银行制度，允许私营机构和私人发行货币并自由竞争，以浮动汇率买卖，在这个竞争过程中发现最好的货币——任何能够保证稳定购买力的货币，将淘汰市场上其他不太稳定的货币。发币企业追求利润最大化和市场竞争的过程会带来一个高效的货币系统，其中只有稳定的货币才能生存。

弗里德曼著有《货币的祸害》。在他看来，小岛上的居民的交易只在石币上画记号，与现代货币体系下的交易并没有什么不同。货币体系不一定需要强权政府的信用支撑，何况这种信用本身也不一定可靠。弗里德曼比哈耶克幸运的一点是，他生活在技术时代。所以，其理念比哈耶克的“在竞争中

发现最好的货币”在技术上（不涉及理论）更进了一步，他构思了一个用技术程序来发行货币的想法，以限制央行的货币超发。

弗里德曼在2006年去世，比特币在随后的2009年诞生。若是弗里德曼还活着，也许能写出《新的货币时代》。弗里德曼的儿子说，我父亲将会对比特币非常感兴趣。假如门格尔、庞巴维克、米塞斯、哈耶克也都还活着，虚拟货币和比特币这件事情将会变得非常有趣。

对于通货膨胀和经济周期的担忧是这几位学者研究货币生产的经济与伦理的出发点之一。他们思考着不让某一方控制货币的发行，保护私有财产，维持金融秩序稳定。真的有必要让政府控制货币吗，尤其是在脱离金本位以及动动电子数字就能发行货币的时代？弗里德曼基于对货币史的研究，认为政府并不那么可靠和值得信任。而在货币发行上，政府也不是必要的参与者（但是不意味着不能参与，法币与私企、个人发行的货币也可以是竞争关系）。

货币价值并不捆绑国家信用，货币可以非国家化。在以前的贝壳和黄金时代，我们就是这么做的。但是，用什么方式来替代它及其身后所谓的国家信用呢？是哈耶克的“在竞争中发现最好的货币”、弗里德曼的“让技术系统发行”，还是现在听起来甚至可能是个笑话的比特币？其实三者并不矛盾。

虚拟货币，尤其是比特币，几乎就是承袭这一思想量身定做的，而又有所突破。哈耶克提出的设想类似于私人机构的可充分流通的无息债券，打破了法币的壁垒；弗里德曼提出的让技术系统发行，则引发了“货币是否需要金本位或者其他一定实物价值背书”的质疑。

假如货币本身只是一种过程协议，主要作为价值尺度和流通工具的话，那从源头上是不必要求其必须与实用价值的货物捆绑在一起的。前提是，这种货币得到充分的信任，而价值自然在交易中产生。但是充分的信任不容易获得，所以历史上自然地衍生出了金本位等制度。

比特币也许有机会获得这种充分信任。任何一种去中心化的货币都有机会，因为它接受的就是公众的契约和监督。即使比特币目前来看比与它相似的山寨币更有机会获取信任，但比特币或许最终也会失败。不过，分布式、去中心化的思想必定会影响未来的货币体系和支付方式。

至于其他虚拟货币，无论传统的还是新型的，无论是内部流通的还是可以在市场充分流通的，都可以在未来扮演角色。比特币也非法币，不存在强制的非此即彼的问题。在竞争性生产货币中——最被公众信任的那几类，也可以在小生态中使用其他虚拟货币。

价值支撑

在弗里德曼去世3年后，比特币出现了。互联网的思想、技术的进步是时代赐予我们的最好的礼物。货币是经济金融最重要的领域之一。在货币领域，或者说是记账系统和交易领域，比特币的出现让人震惊，虽然其现在的规模与全球货币体系相比仅仅是九牛一毛。

不是权力机构或者人，而是冷冰冰的数学公式和代码带给我们温暖的契约和理性的思考。比特币在这一点上登峰造极。

比特币是一种点对点的电子现金系统。事实上，它符合弗里德曼描绘的让技术系统发行货币的想法。一组“挖矿”的程序自发产生货币（或者说不断更新账户体系），并且受到总量的控制。这套系统去中心化，基本不能被人为控制，除非有人控制了系统中50%以上的运算能力。

即使某人真的达到了这样的运算能力，对系统的安全性而言，“挖矿”也是一个非常可靠的程序，因为它提供了诚实行事的动机。“如果一个贪婪的攻击者能够比所有诚实的节点聚集更多的算力，他将不得不做出选择：用它来欺骗别人并偷回他已经支付的款项，或用它来生成新的货币。他应该会发现按照规则行事更有利可图，这样的规则会让他得到比其他人加起来还多的钱，这样他就不必破坏系统以及自己财富的有效性。”

这样的条件看起来非常完美，但即使总量恒定、技术完美，比特币的价值在哪儿？它为什么值得信任？

价值存在于共识（信任）和交易本身。不是为什么值得信任，而是你是否选择信任。之前的社会信任都是基于一定的实际效用和货物或者国家政体而产生的，而比特币是基于去中心化、总量恒定的特点而自发产生的社会契约信任。基于实际效用和国家政体与基于理念产生的信任相差太多，但是两者不能相互否定。把选择权还给社会和公众即可。

假如说共识和社会契约就能够形成价值，那可能还是太虚无缥缈了。很多人认为挖矿本身是不提升整体社会效用的，所以没有价值。没有价值的东西怎么可以作为交换中介？（与此矛盾的是，他们居然认为纸币有价值。）

事实上，虽然比特币系统的经济学原理源于奥地利学派，也得到了他们的支持。但是，部分奥地利学派经济学家也同样质疑比特币。这种质疑来自于：比特币没有内在价值，并不符合米塞斯回归定理。他们认为，货币被接受不是因为政府法令或社会惯例，而是因为它根植于有一定购买力的某种商品中。

那么，货币需要资产支撑吗？比特币和其他虚拟货币还不一样，其他虚拟货币往往存在对应的虚拟服务的预付，也算是广义上的资产支撑了。哈耶克也曾提出，在竞争性生产货币中，货币需要一揽子商品标的支撑。“货币是需要兑现的。”

但我们不要忘了，比特币的实质和核心是一种交换媒介和记账单位，并无黄金般的实物价值及其他满足社会效能的价值。价值可以只是存在于交换媒介和记账单位本身，使交易变得高效、方便、安全，保护私有财产……难道还不够有价值吗？为什么一定要在交易之外寻找价值和兑现呢？在货币价值中，这两者是最重要的。是的，没有交易，黄金狭义上还有使用价值，但比特币就没有价值了。但是，那又如何呢？极端的假定是没有意义的。当然，若把比特币当成一个记账系统而不是货币，可能更容易理解其价值。

去中心化有助于实现货币民主，保护私有财产，使交易高效、便捷，避免双重支付……已经足够有价值了。

虚拟货币新时代

也许，在虚拟货币新时代之前，我们应该回答一个问题：虚拟货币有新时代吗？它会不会因不易控制而被政策扼杀？对于政策，我们不做揣度。但是在技术上，虚拟货币是无法被消灭的。

抛开上面那些虚拟货币的优势不论，只要互联网存在，虚拟货币就有存在和发展的空间。货币与支付是紧密联系在一起的。互联网技术的发展使得支付可以脱离中央银行的清算系统。支付已经成为不依赖于中央系统的私人选择领域。那么，用户和市场选择使用什么中间媒介，中央银行是无法捕捉和干预的，除非公权力全面入侵私人领域。

笔者想在虚拟货币的基础上提出一个更细化的概念——互联网货币，也就是上文所论述的新型虚拟货币。互联网货币不是基于虚拟社区产生的虚拟货币，而是在互联网平等、高效、共享、去中心化的思想基础上建立起来的。只要存在特定发行人，平等和去中心化就没法实现。平等和去中心化的意思是，每个人都拥有发行和流通货币的自由。比如就比特币而言，谁都可以是发行人。

互联网货币就是虚拟货币新时代。在此基础上，也许我们可以在货币和支付上找到通畅之路。

08 比特币的未来

假如斯诺登生活在2023年

2013年6月，一名29岁的男子自夏威夷飞至香港，拖着一个小黑行李箱，里面藏有4台电脑，正是这4台电脑让他数周后为全世界所知。这名男子正是爱德华·斯诺登，因曝光了美国“棱镜”秘密情报监视项目而名噪天下。但他后来曾一度陷入窘境：9日，冰岛驻华大使表示，冰岛无法为斯诺登提供庇护。10日，媒体报道称斯诺登“快要用光现金”，由于酒店的昂贵开销，他的信用卡很快就会透支。11日，他退房了，去向不明。15日，有香港立法会议员建议斯诺登主动离境，或者等待被引渡出境……

一个大胆的设想是，如果这一事件推迟10年，发生在比特币大行于世的2023年，又将是怎样一种情景？斯诺登是一位计算机高手，精通密码学和编程，是一个理想的比特币极客。在媒体细致入微的全方位报道下，我们

对斯诺登的逃亡细节有了大致了解。现在，只需对这些细节做一些智力推演。令人惊讶的是，我们得到了完全不同的情景，让我们开始吧！

2023 年 1 月，斯诺登通过比特信（Bitmessage）[①] 与伦敦、莫斯科方面的神秘联系人秘密接触，他们并不相信他握有具有价值的情报。斯诺登给他们发送了一个比特币交易ID（身份标识号码）。对方通过交易ID很快破译出用SHA–256 消息摘要编码的情报，情报透露了美国于 2022 年 6 月在伊朗发起的一桩军事行动，这个情报显然不是伪造的，因为交易ID的时间戳显示是 2022 年 5 月，比这次行动足足早了一个月。伦敦与莫斯科方面的态度有了 180 度转变，都表示将为斯诺登提供政治庇护。

斯诺登要求签订一个三方协议，由他创建一个比特币三方交易，发送到伦敦与莫斯科的比特币地址，该交易只有在伦敦与莫斯科都用私钥签名后才能生效，协议内容用比特币标准三方协议格式编码，该协议被比特币全网广播后的结果是，若斯诺登前往英国或俄罗斯并提供有价值的情报，那么他将得到两国的政治庇护。由于英、俄两国情报机构的官方公钥是公开信息，任何人都可以核实这两个公钥分别属于伦敦与莫斯科。在协议的约束下，伦敦与莫斯科都不会贸然违约，因为一旦违约，斯诺登可以向社会公布这个三方协议，在全球拥有大量雇员的英、俄两国的情报机构的诚信将严重受损，这显然不符合两国的利益。

① 比特信是一种P2P加密通信软件，其通信原理类似于比特币协议，可防止窃听者通过运行未经授权的程序来监听消息。

6月，他飞抵香港。此前与他接触过的《卫报》等媒体如约而至，斯诺登向其揭露了“棱镜”计划的细节，举世震惊。伦敦方面也大为震怒，因为斯诺登原本的承诺是只向伦敦提供情报而不是公之于众。伦敦方面拒绝为斯诺登提供资金。没了资金赞助，斯诺登并不惊慌。逃亡前他已经将资产换成了比特币。他还向几位陌生人贷了几百比特币，以房产和汽车作为抵押。房产和汽车都内置了所有权密钥，贷款后他仍拥有对所有权密钥的访问权，所以这并不妨碍他的女友继续使用他的住房与汽车。他还留下遗嘱，用SHA-256消息摘要编码进比特币区块链。遗嘱表示，他若有不测，其资产全部留给女友。

香港美丽华酒店的每日房价高达500美元，坚持了几个月后，斯诺登的比特币资金有点儿紧张了。更重要的是，他每个月都必须向债权人的比特币地址打钱，若逾期不还贷，其房产和汽车的所有权密钥将自动更换为债权人的。他想向莫斯科方面出售情报，但莫斯科不相信他手上还有什么未公布的情报。要证明自己确实还有秘密并不难，但要提交情报后确保对方如约给钱却很难。于是，斯诺登把情报转化成零知识证明的程序，然后给莫斯科方面提供加密的情报（Ex）、解密密码K的哈希（Hk）以及情报程序的运行结果（Y），对方可以通过Ex、Hk、Y三个参数验证程序运行正确，但无法知道情报的具体内容。莫斯科方面验证程序后，决定购买情报。莫斯科用斯诺登的公钥（比特币地址）创建一个付款，斯诺登必须给莫斯科披露密码K以换取这笔付款，莫斯科需要用K来解密Ex并获得情报。交易确认后，斯诺登得到

比特币，莫斯科则得到K，在此过程中，双方都没办法欺诈，彼此并不需要建立信任。

就这样，斯诺登在三方协议的保护下，安然无恙地生活在香港的某个酒店，没有被引渡的危险。他用匿名的比特币支付房租，因而也没人知道他究竟在哪里。中央情报局根据斯诺登的抵押贷款确定了一个属于斯诺登的比特币地址，但是很遗憾，这个地址没有办法追踪，因为斯诺登使用了一个叫零币的服务，把比特币在池子里混合后，就不知去处了。斯诺登手上有多达6G的绝密数据，他把其中最重要的那部分数据压缩加密，打包编码进了比特币区块链，硬盘早已销毁。密钥转化成了一个只对他有意义的句子，记在脑海里，没有人能偷去。比特币网络的强大算力可以保障这些数据永久保存且不可修改。靠分期分批向莫斯科和其他国家出售情报，他能一直惬意地生活下去。他还用比特币给远在美国的女友买了别墅、保时捷。

在这个想象的故事中，斯诺登分别用到了存在性证明、零知识有条件付款、零币、分布式合同、智能资产等比特币应用。很难想象，黄金、白银、信用货币等能实现如此多的智能经济行为。比特币还原的只是货币的本质，因为人们原本只需要不可复制、不可滥发且可零成本转移的信息而已。人们说，金银天生是货币，现在，中本聪给这句箴言添加了新的注脚：货币天生是信息。正因为它是信息，我们才可以轻易地用比特币实现无数经济行为与金融工具。太平洋雅浦岛的居民使用石币贸易时，他们并不需要把屋前屋后的石币真的搬到对方的家，而只需在石头上做个标记，并向全岛通报，这块

石头现在属于对方了，这与比特币通过P2P网络广播交易信息并无二致。正如美国明尼阿波利斯联邦储备银行主席纳拉亚纳·科赫拉科塔在1997年说的："货币不像普通人所理解的那样，是一个价值存储工具、一个交易单位或者记账单位，而是一个技术上的具有集体记忆功能的工具。"而现在，他所预言的那个具有集体记忆功能的工具出现了！

比特币的开放性

信息不对称催生了对冲基金、房地产经纪人、借贷担保、银行等各种中介，它们知道更多不为人知的信息，人们付费请他们做自己想做却无从下手的事情，它们从这种不对称中获得利润。而在比特币经济中，因其公开透明的账单保存机制与难以摧毁的去中心化架构，银行、房地产经纪人、投资代理等各种中介根本无用武之地。人们可以在最低信任度的情况下，通过比特币网络完成合同签订、遗嘱执行、数据或资产所有权证明、远程交易、P2P借贷等各种经济活动。而这一切都是建立在比特币网络开放式的应用编程接口之上。比特币提供了3个层次的开放性。

交易行为的开放性

比特币鼓励交易层级的创新。一个典型例子是M-of-N签名脚本，这种交易允许用N个密钥中的M个签名解锁。这样一来，企业在需要动用资金时可以采用两个或更多签名，例如一桩交易（资金输出）须经首席财务官、出纳

员、审计员三者中的任意两者的密钥签名方能解锁，从而实现联名账户或受托人/执行人的资金管理。

此外，比特币通过协议的升级，可从目前的点对点交易转变为群对群的三方或多方交易，这对分布式合同具有重大意义。现实经济中经常需要大量用到三方或多方合同，而比特币不可更改的区块链既可保存交易总账，又可编码任意数据的 SHA-256 消息摘要，这意味着人们可以在最小信任度的前提下达成协议，而无须公证员、担保人、律师等第三方的介入。

交易总账的开放性

比特币网络允许节点之间相互通信、转发交易、验证新的交易区块和生成新的比特币。所有这些网络协议的交互，使得每个节点都可以构造出共享交易总账的一个完整的、一致的本地副本，即区块链。比特币交易总账的开放性使得每个人都可以提供涉及比特币交易信息的服务。例如，通过告诉你的税务会计师哪些比特币地址是属于你的，他们就能轻松地在总账中找到与之相关的所有交易，并计算出你的收益和损失，甚至为你的比特币交易活动创建最佳的税务策略。经济学家则可以轻易地摸清随时间推移的比特币交易次数变化情况、比特币的平均交易规模、任何一个时间节点上实际流通的比特币占全部比特币的百分比等。

这实际上相当于三方记账法，因为每一笔经济业务除了以相等的金额登记在两个（点对点交易）或两个以上（群对群交易）的账户中外，它还永久

保存在以时间戳为刻度的区块链上。如果说1494年由圣方济各会修道士发明的复式记账法使企业监控资金流动、操作复杂的资金业务成为可能，并造就威尼斯银行业的繁荣，进而开启了资本主义的大门，那么，比特币三方记账法的诞生必将更加深远地影响全球经济，因其与计算机技术的无缝对接既大大降低了会计与审计成本，使得追踪财富流动更廉价高效，其账单不可修改的特性也杜绝了出现假账、错账的可能性。

一个典型的应用便是使用比特币募捐，公众可以通过观察比特币募捐地址上的资金去向来推断这些捐款的相关用途，再也不用担心捐款悄悄进入私人腰包。捐款者也不会再有被质疑诈捐的烦恼，因为他只需用私钥对募捐地址进行消息签名，即可轻易地证明某笔捐款确实来自自己。

钱包数据的开放性

通过比特币客户端的远程过程调用中间件协议（JSON-RPC）可将整个比特币经济公开。这种API（应用程序编程接口）提供的服务包括查询钱包余额（相当于查询比特币世界的银行账户余额）、创建交易、创建新钱包等。你可以通过代码查看你的余额或其他任何账户的余额。你可以在一个公平的环境里创建信息并交易。你可以独立运作一家银行、证券交易所、电汇服务或担保服务，而不需要任何人的许可和认证。正如互联网让每一个自媒体都有能力达到《纽约时报》的读者量，比特币则让每一个节点甚至是运行在你手机的节点，在能力上等同于富国银行或美国银行。

比特币未来协议扩展与应用

比特币既是一个潜力巨大的基础性平台，更是一项开放式P2P交易传输协议。其开放性和架构性甚至较STMP、HTTP、RSS以及BitTorrent等协议有过之而无不及，开发者、企业家们正在开发基于比特币协议的新技术、新应用，目的是使它更安全、更便利、更全能。

存在性证明

存在性证明是指把数据文档的SHA-256信息摘要嵌入比特币区块链来证明其存在性。其原理是通过两个编码过的且包含哈希的特殊地址创建一个有效的比特币转账，这个哈希被切成两个片段，每个片段包含这些地址之一。哈希片段用来替换椭圆曲线数字签名（比特币地址生成算法）公钥的哈希，这些特殊的转账之所以不能花费，正是因为这些地址是由文档的片段生成的，而不是由椭圆曲线数字签名算法的私钥生成的。

地址生成且交易确认后，该文件即被永久认证。只要交易被证实，则意味着该文件存在。如果文件在交易时不存在，它不可能在两个地址中嵌入其SHA-256消息摘要并创建转账（因为哈希函数具有抗第二原像性）。由于哈希函数的抗原像性，试图嵌入一些哈希散列，以与未来的文件哈希值相匹配也是不可能的。这就是为什么一旦文档所产生的转账被比特币区块确认，该文件的存在性就被证明了，而不需要一个值得信任的中央权力机构。

如果有人想在时间戳上手动确认文件的存在，他们应该遵循以下步骤：

1. 计算SHA-256 信息摘要；

2. 找到比特币区块链上的转账记录，给文档的地址发送比特币；

3. 反编译Base58 编码的地址；

4. 嵌入摘要，替换这两个地址的公钥哈希，由于摘要共有 32 个字节，而每个地址可容纳 20 个字节，剩下 8 个字节用零填满；

5. 区块链上这两个地址间的转账可证明该文件在那个时间确实存在。

存在性证明的主要用途包括：在不透露实际数据的前提下展示数据所有权；证明某些数据在某一时刻的存在性；检查文件的完整性。

零知识有条件付款

在文艺复兴时期，意大利的两个数学家塔尔塔里雅、菲奥为争夺一元三次方程求根公式发现者的桂冠而闹得不可开交。他们都宣称自己发现了这个求根公式，但谁也不愿意把这个公式公布出来。于是，他们摆起了擂台：双方各出 30 个一元三次方程给对方求解，谁能全部解出，就说明谁掌握了这个公式。比赛结果是塔尔塔里雅解出了菲奥的 30 个方程，而菲奥一个也解不出。于是，人们相信塔尔塔里雅是一元三次方程求根公式的真正发现者，虽然当时除了他本人外，谁也不知道这个公式究竟长什么样。这种既能充分证明自己是某项权益的合法拥有者，又不把有关信息泄露出去的方法就叫零知识证明，即提供给外界的“知识”为“零”。

零知识证明早在1986年就被A·菲亚特和A·沙米尔用数学方法给出了解决方案，并在同年申请了美国专利，但由于该理论可能被用于军事领域，专利局被军方密令禁止发表，理由是："该申请发表后会有害于国家安全……所有美国人的研究未经许可而泄露将会被判刑罚款。"这一禁令闹了个大笑话，因为作者实际上是在美国申请专利的以色列人，研究也是在以色列的大学里完成的。此次乌龙事件也从侧面反映了零知识证明的重要性。

如果把零知识证明与比特币联系起来，你可以实现零知识有条件付款。设H（）是一个复杂的计算机程序，对于H（X）=Y，给定一些特定的Y，你想推导得出符合条件的X。H（）也可能是一个密码哈希算法，给定一个特定的哈希，让你破解哈希进而找到那个密码。又或者H（）是一个复杂的程序，Y的值取决于你找到一个漂亮的图形。

如果我碰巧知道问题的答案，即那些符合条件的X，并想把答案卖给你，但是我们相互之间并不信任，由于我们身边都没有朋友，所以也没有谁能充当调解员。我们是否可以在零信任度的情况下使用比特币交易呢？答案是肯定的。

数学上已经证明：你可以将任何计算机问题转化为零知识证明问题，因此，使用零知识证明的确可以证明自己知道一些X，使得H（X）=Y。但仅有零知识证明还不够，因为你付钱给我之后，我可以不告诉你答案，或者，我告诉你答案之后你又不付钱了。所以，我们需要引进加密交易。

我用随机密码K加密X，Ex=AES（X，K），然后，我构建程序：

```
Program（K，Ex，H（））=> [Ex，Hk，Y]｛
```

```
    Hk=SHA-256（K）；
    Y=H（UNAES（Ex，K））；
    return [Ex，Hk，Y];
}
```

这段程序使用随机密码（K）对解决方案进行加密，再输出加密的解决方案（Ex）、随机密码K的哈希（Hk）以及解决方案程序的运行结果（Y）。

我将这个程序转换成零知识证明，从比特币外部告诉你Ex、Hk、Y，然后你可以用这三个参数验证我的确能诚实地执行这个程序。

然后你需要我的公钥（比特币地址）和密码（K）来创建一个比特币付款，我必须向你披露密码K以换取这笔款项，你需要用K来解密Ex并获得解决方案。这样一来，我们任何一方都不能欺诈，所以这个过程中我们并不需要互相信任。

目前，这个方案尚未被广泛使用，因为并不是所有人都能弄明白在实践中怎么应用。

彩色币

通过跟踪一些特定比特币的来龙去脉，可以将它们与其他比特币区分开来，这些特定比特币就叫作彩色币。它们具有一些特殊属性，比如支持代

理或聚集点[①]，从而具有与比特币面值无关的价值。彩色币可以用作替代货币、商品证书、智能财产以及其他金融工具，比如股票和债券等。

比特币的P2P支付结算系统已经安全建立，可以实现可靠的、近乎免费的转账，比特币网络（协议）本身是安全、稳定的，但比特币生态的服务提供商（比如汇率市场）却多次被黑客攻击，损害了比特币的声誉和交易价值。有没有一种办法可以利用安全可靠的比特币自身协议创建分布式的汇兑交易呢？

BitcoinX就是这样一个基于比特币的开放标准协议，用来规范互联网的价值交易。基于BitcoinX协议，你不但可以在分布式、安全的云平台上持有比特币，还可以持有黄金、欧元、美元和各种证券资产。这意味着人们可以使用金融工具自由交易，如果某个节点G持有黄金，另一个节点E持有欧元，它们可以以一种安全、透明、直接的方式相互兑换，而不需要第三方的介入。

BitcoinX的设计思想是将比特币网络（技术）与货币价值分割开来，并使用比特币网络技术明晰交易来路以避免重复消费。通过创世转账建立一个新货币（即彩色币），创世转账是指一定量的比特币转账，这些比特币金额将用来赋予所有这种新货币价值。这一定量比特币发送到的那个地址就是新货币的起源地址，它将控制新货币的初始分配。

彩色币客户端就是通过一种特殊的方法计算资金平衡的轻量级客户端。

① 聚集点（Schelling point）是指在博弈论中，人们在没有沟通的情况下的选择倾向，做出这一选择可能因为它看起来自然、特别或者与选择者有关。

所有转账的最后一个地址就是客户端地址，我们抓取区块链，查看这些转账是否来自创世转账。如果是，我们用交易金额乘以初始分割率就可以得到用户余额。

初始分割：0.000 01BTC = 1 彩币（假设值）

彩色币客户端是分布式的，然后围绕特定的创世转账创建一个社区，这就创造了一个与比特币网络无关的独立的彩色币生态，这个小型经济生态的波动建立在对比特币的基础设施的利用之上。

由于彩色币也是普通比特币，所以它们也可以通过比特币网络从一个地址传送到另一个地址。因为我们有办法识别彩色币，所以它们相当于稀有货币，其价值取决于用户对这种稀有货币的需求，而与比特币价值无关。

彩色币怎样进行初始分配呢？在货币创世时，彩色币起源地址拥有该币的总体价值。在分配结束时，所有的货币价值将从起源地址转移到每个客户端。

在实际应用中，彩色币拥有者将不会知道货币总量有多少，拥有者也不必知道想参与他的经济的人有哪些。他可以建立一个邀请系统，每一个新的客户端都可以邀请其他客户端加入。实现这种技术还有很长的路要走，比如社交网络身份验证、社会图谱搜索、担保系统、短信验证、独特的IP地址（互联网协议地址）、物理识别等，这些方法可最大限度地减少初次分配中的欺诈。

零币

零币（Zerocoin）是一个比特币的建议扩展，它可实现真正意义上的匿名性。正如历史上纸币因可兑换黄金而建立了价值，零币也因可兑换比特币而建立起自己的价值。

比特币的交易记录是完全公开的，所有人都可以通过你的钱包地址在区块链中查询你的钱包现金流入与流出，并可向上追溯至这些比特币的终极起源，即区块生成后发送到的那个地址。这对个人隐私构成了极大威胁。

比特币协议为上述问题提供了两种解决方案：所有的比特币交易使用公共密钥，而无须个人身份证明，或比特币客户端可以生成无数个公共密钥，以帮助用户摆脱跟踪。然而，越来越多的研究表明，这些保护措施是不够的。如果通过一些社会工程学手段，使得某个比特币钱包的物理地址（如IP地址）暴露，再配以大数据分析，那么，资金的来龙去脉与关系网将无所遁形。在《大数据时代》一书中，作者用例子证明了大数据分析的威力：通过对美国在线 2006 年 8 月公布的 2 000 万匿名搜索查询记录的分析，《纽约书包》发现，数据库中的 4417749 号样本代表的是佐治亚州的一名妇女。

为此，约翰 · 霍普金斯大学的密码学研究小组在 2013 年 5 月的“IEEE（电气和电子工程师协会）安全和隐私大会”上提出了“零币模型”，主要提供一种洗币服务，用来混合比特币的交易历史。它创建一个与比特币区块链并行的匿名货币，以固定面额发行，任何用户都可以用比特币购买零币，这种交易是通过一种叫作“零币铸造”的特殊块链进行的。

一旦铸造交易被比特币节点接受，该用户就可把零币兑回比特币。他只需简单地把比特币接收地址（最好是新生成的）嵌入“花掉零币”的交易，然后发送到网络即可。如果交易被确认，比特币节点会将它视作一个正常的比特币转账。这意味着他的比特币接收地址将收到等额比特币（减去交易手续费）。

这个过程的关键在于，接收到的比特币与起初使用的比特币是毫无关联的。通过使用各种加密组件，包括数字签名和零知识证明，实现的效果是，不可能在数学上建立接收到的比特币与起初使用的比特币之间的联系。

合并挖矿

比特币区块链有几个替代用途，包括使用区块链作公证服务（比如，存在性证明把一个哈希分割成两个，并创建一个不可花费的输出），又比如小额支付和彩色币，也引发了对这些新协议加入比特币区块链的担心。

一个解决方案是创建其他区块链，如果该区块链是与比特币网络完全独立的，一个全新的哈希网络就诞生了。不过，若采用中本聪与比特币开发者迈克 · 赫恩最近讨论的“合并挖矿”（Merged Mining）的设想，则可允许区块链在同一网络同时挖不同的矿。

比特币工作量证明机制是指在矿工挖矿时，给区块补增一个随机数，并开展随机哈希运算，使得给定区块的哈希值开头含有一定数量的零。

假设对“message”（不含引号）进行SHA-256 算法加密，你会得到：

ab530a13e45914982b79f9b7e3fba994cfd1f3fb22f71cea1afbf02b460c6d1d

现在开始加入数据，直到你得到一个以 0 开头的哈希：

1message daad0bc80059253928621a10365de153e335a18f03b9dc7e7e25897fb791f023

2message 6532f42bd1d6ccd00f47c133c3ca1a0fc852598e67c62eb31adab8ceb3aaa680

……

51message 0985e57510d017b177867168642543ab4f143333ad63782680e812251ab3141e

51 次运算后得到了第一个有效的哈希。只要“51message”一发送，接收器可以迅速通过哈希运算来验证它是否符合要求。被添加的那部分数据（本例中的“51”）被称作随机数（nonce），关键在于该随机数可以是任何信息。

假设你在同时挖A币与B币，现在你有部分区块数据来自A币，部分区块数据来自B币，而且一个母随机数会不断改变，直到你找到一个区块。一旦你找到一个块，它就是一个对A币、B币同时有效的块链（假设两者的挖矿难度相等）。

同时哈希以下数据：

[A币区块数据|B币区块数据|公随机数]

当一个块被发现：

对A币广播区块>>[A币区块数据]+随机数=B币区块数据+母随机数]

对B币广播区块>>[B币区块数据]+随机数=A币区块数据+母随机数]

只要你愿意，你可以制造任意多的链。Slush矿池2011年就已经合并挖比特币与域名币。

合并挖矿的好处包括：同时为两个区块链贡献哈希算力，有助于提高两个区块链的安全性；挖矿的回报更高，在消耗相同电力的情况下，可同时采两种货币，如果你不喜欢域名币，可以把它换成比特币。

域名币

域名币是一个基于比特币技术的分布式域名系统，提供.bit等后缀的域名注册服务，具有安全和抗审查特性。域名币的原理和比特币相近，其区块链独立于比特币区块链，但可通过合并挖矿来运行。域名币的顶级域名没有一个中央机构或组织来管理，每个域名币节点都保存有一个数据库副本，允许用户使用备用DNS、DNS后缀、网关、浏览器插件或安装域名币客户端获得独立的取得认证的域名浏览权，在使用客户端的情况下，没有任何权力机构可以禁止域名的使用和转让。

注册一个域名币域名的花费由网络费用和手续费两部分组成。这些费用通过域名币支付，初次注册需要花费50域名币，每两个月网络费将减少1/2，这就意味着一年内网络费将慢慢少于1域名币。之所以开始需要缴纳较高的网络费用，是为了抬高早期注册门槛，以确保后期仍然有足够的域名，但随着时间的推移，域名的网络费用会缩减到忽略不计。这笔网络费不会流到任何人的手中，因为在交易过程中它会被销毁。而手续费将付给

矿工们，与比特币类似，挖矿之初付多少手续费由你来决定，可以是 0.01 域名币甚至是免费，不过付费越高，交易处理的速度就越快。大约每 3 个月你需要对你的域名进行一次升级，不过这个过程是免费的。升级的方式是通过你的域名账户内所绑定的域名币作为输入，产生交易从而升级，账户中被内置了特殊的 0.01 域名币，这种特殊的货币不能用来交易，从而保证你的账户不会被清零。

Dot-BIT是第一个使用域名币的项目，旨在建立以.bit 为后缀的DNS系统。目前该项目仍然处于测试阶段，已有 7 个DNS服务器，域名数目已超过 7.9 万个。

分布式合同

如果多方交易功能被添加进比特币核心代码，那么比特币将不仅仅是货币。现在，加密货币的开发者正在设计初步支持新型交易方式的模型。

什么是多方交易？多方交易让分布式合同（Distributed Contract）得以实现。分布式合同是一种人们通过比特币区块链达成协议的方式。分布式合同并不能实现以前的合同所不能达成的功能，它只是促使人们在最小信任度的前提下达成协议。这意味着以前只能以在纸上签字的方式达成的协议，现在可以在密码学的信任基础上完成同样的服务。这种新服务可以开发出托管服务、抵押贷款、纠纷调解、买卖担保、智能资产等诸多新功能，这些功能将消除许多行业中需要用到纸质合同的情形。除了银行，可能会受到影响的包括企业冠名、贷款、结算、数字产品（汽车、手机、电脑）的所有权转移、

资金服务等，以比特币的方式创建这些合同的成本几乎为零。

假设有A、B、C3个人，新的交易形式可能包括以下几种：A和B、A或B、A和B或C。比特币并不仅仅是一种全球货币：目前，它可以取代纸质的现金；将来，它也许可以取代许多金融行业内的纸质合同。比特币可能是世界上第一个全球加密合同协议，任何人都可以在世界的任何地方，以加密的方式与任何人做生意。

智能资产

智能资产是指通过协议用比特币块链来控制财产所有权，比如汽车、电话、房产等实物财产。智能资产还包括非物理属性的财产，比如公司股份、某计算机的远程访问权限等。智能资产允许在最低信任度的情况下进行交易，这消除了欺诈与中介费，并允许交易发生在用其他方式不可能实现的领域。比如，它允许你向陌生人借钱并用自己的智能资产作为抵押，这使得贷款更有竞争力且更实惠。

智能资产的概念由尼克·萨博于1997年在其论文《关于智能合同的设想》中首次提出，但这个设想暂时还没有实现。

智能资产的原始形式已经很常见，如果你拥有一辆汽车，通过一个协议交换装置，就可以使只有持有加密令牌的人才能启动发动机。这大大降低了汽车失窃率，例如，澳大利亚有45%的汽车安装了防盗装置，只有7%的防盗汽车被盗。

让我们继续以汽车为例来理解基于比特币协议的智能资产。车载电脑需要一个所有权密钥来验证身份，所有权密钥是固定的比特币ECDSA-256密钥。汽车出厂后创建一个新的所有权密钥作为其使用生涯的开始，一小笔比特币存入该密钥地址，称作调用量T，可以是0.000 1比特币。此外，汽车还拥有一个来自制造商的数字证书，证书中包括验证身份所需要的公钥，这允许汽车向第三方证明其存在、使用年限或行驶里程等。

当汽车被出售时，使用以下协议：

1.买方生成一个随机数，并要求卖家发送汽车数据。

2.卖家向汽车输入该随机数，汽车返回一个用身份密码签名的数据结构。该数据包括汽车的证书、汽车的数据、当前所有者的公钥和最后一次交易的merkle树[①]。这可以让买方确保这些数据的确来自卖方，且不是一车多卖。

3.卖家创建一个密钥作为收款地址，记作K_1，售价记作P。

4.买方生成一个新的所有权密钥，记作K_2。

5.买方创建一个有两个输入和两个输出的交易。输出一给K_1发送P个比特币，输出二给K_2发送T个比特币。这桩交易是无效的，因为只有第一个输入可以签名。买方把这部分完整的交易传给卖家，卖家再用汽车现拥有者的私钥对输入二进行签名，并向全网广播这桩交易。

6.等待确认。

① R·C·默克勒于1980年提出的一种区块压缩方法，只有根被纳入了区块的随机哈希，树的分支则被拔除，而内部的随机哈希是不必保存的，这样区块大小会被压缩。

7.买方通过比特币交易取得汽车的所有权。一个merkle 树连接了区块头，很快有足够多的区块头验证了汽车目前的这桩所有权交易。汽车发现这桩重新分配所有权的交易所在的区块链比当前的链条更长，就会将这桩交易添加到其工作量的顶部，以确保该交易不发生逆转。然后，它会更新所有权信息，这辆车并不需要完整的区块链记录，也不需要全部区块头，只需足够多的数据保证目前已有的区块头可以连接到将来的区块头。

在现实中，这与智能手机使用NFC（近距离无线通信）硬件的过程很像，用所有权密钥加密屏幕区域，以特殊方式触摸智能手机可以启动具有智能资产交易功能的钱包应用，通过输入价格，买方和卖方同时触摸自己的手机来完成交易。虽然加密技术本身非常复杂，但使用者根本不需要懂得加密。

贷款与抵押

智能资产使我们能够买卖实物财产，且没有欺诈风险，这大有用武之地。但有时候，人们除了买卖实物资产，还需要向陌生人借贷。我们可以通过添加一个附加层来实现低信任担保贷款。以贷款做小生意为例，如果你决定让来自世界各地的人对你的债务进行出价，而不是与银行打交道，这样你就可以得到最优惠的贷款价格。对于这项业务，陌生的债权人需要一些保证，若你偿还不了贷款，他们将得到抵押品，比如你的汽车，但你仍然需要使用汽车做生意。这该怎么办？

为此，我们可以添加对所有权密钥的访问密码，然后用所有权密钥对

消息进行签名，访问密码可以添加或删除，而且具有临时性。这意味着到了还贷期，你可以重新分配汽车的所有权给债权人，同时又保留自己的访问密码。如果债务人保证偿还贷款，汽车所有权会恢复到他名下，这当然是最理想的借贷。我们可以通过如下方式实现：

1. 债权人生成K_1，它用来接收还贷，贷款规模是L。

2. 债权人用SIGHASH_ALL和SIGHASH_ANYONECANPAY指令给消息Tx_1签名，该消息拥有一个重新分配汽车所有权给债务人的输出/输入，以及一个把总量为L的比特币发送至K_1的输出。此项交易是无效的，因为贷款尚未偿还，故以比特币计价的总输出大于输入。债权人把这项交易发送给债务人。

3. 当债务人赚回了贷款，他们向Tx_1充入比特币以增加其价值。这不会破坏用所有权私钥签名的输入/输出，因为还贷交易是用SIGHASH_ANYONECANPAY 签名的，所以它与其他输出是独立的。他们不能调整以及输出这桩交易的任何数字，否则所有权私钥签名的输入/输出（所有权交易是用SIGHASH_ALL签名的）交易将失效。

4. 一旦交易的输入达到了L，债务人就广播这桩交易，从而偿还其债务，同时取回汽车所有权。

由于访问密码设定了时间限制，如果债务人逾期无力偿还贷款，他的访问密码将过期，该车将不再属于他。新的所有者可以取走它，如果不想取走这辆车，还可以使用低信用买卖协议（智能资产）卖掉它。

大部分贷款是分期偿还的，上述协议可以通过嵌入一些额外的输入/输出，让新签名覆盖“逾期”指令，这样便可将访问密码的寿命延长到下一个月，但并不改变汽车所有权。汽车智能电脑知道如何解译出交易数据。

比特币未来展望

比特币的不确定性

“计算机专家们都失去常识了吗？实际上，没有一个在线数据库可以取代每天的报纸，没有哪个CD-ROM（只读光盘）可以取代启迪心灵的老师，没有一个计算机网络可以改变政府的运作方式。”这是1995年《新闻周刊》上刊登的一篇评论文章，它代表的是变革到来前夕人们对互联网的一个典型观点，当时许多人都认为互联网就是一个噱头，缺少编辑，缺少审核者，就像是一个被粗制滥造的数据填满的海洋。时至今日，这篇文章仍时常被人提起，因为人们需要重温这段历史，警醒自己不要漠视新事物，即使它还处在蹒跚学步的婴儿时代。

有时候，只有某种现实存在已久，人们才承认它是现实。人的大脑是在非常缓慢的原始环境中进化而来的，要适应如此飞速发展的变化的确很难。令人意外的是，一些领域的行业专家、意见领袖也并不看好比特币，甚至持有较深的偏见。但这也是可以理解的，哲学家托马斯·库恩提出范式的概念，他指出科学的实际发展不是事实、理论和方法的简单堆积，更不是知识

的堆积，而是通过范式的不断转换进行的科学革命的交替过程。对大部分情形而言，经验很有帮助，但遇到范式转变时，经验往往是有害的，一张白纸反而更有利。比如很多C语言程序员习惯了函数式的问题分析方法，特别不适应C++这种面向对象式编程，初学者学习C++反而更容易。对于专家们来说，他们固有的知识体系与丰富的经验就构成了他们认识新事物的障碍。佛曰：知见障，所知太多而阻障修道矣。

对传统经济学而言，比特币就像是一只贸然闯入的黑天鹅，它不仅废除了被认为是金融智慧最高成就的中央银行制度，还让建立于信用货币基础之上的高度杠杆化的金融金字塔有了崩塌的危险。正如百万台大规模集成电路击溃由高等祭司所卫护垄断的中央服务器，比特币也将打破金融婆罗门的垄断。对于一种颠覆性的技术，用过去的知识体系来评价它显然有失公允，因为其诞生本身就是为了打破过去的框架，创造新的金融结构与商业模式。

另外，比特币的支持者似乎并不在意质疑声，有些朋友对比特币略知皮毛，就迫不及待地投入全部家当，购入比特币资产或矿机，或辞掉工作投入比特币创业。这种乐观情绪似乎来得太过突然了，就算是历史上那些大获成功的技术产品，如电视、手机等，在爆炸式增长的前期，也都经历过异常艰辛且漫长的历程，更何况一段时间的领跑者未必会成为最终的胜利者，比如网景浏览器。在比特币支持者情不自禁地吹捧其美好，或者比特币的批评者下意识地嘲讽它时，双方都不妨提醒下自己，它只是一个诞生才4年的事物。它起始于粗糙，发轫于不羁，还有太多不确定性供我们探讨与想象。

比特币怎样自我进化

比特币的自我进化建立在 3 点共识上。

对价值的共识：比特币不仅仅是一个货币，它也是一种技术，因此需要正确运行才能保障其价值。

对规则的共识：参与者决定哪些交易规则是被允许的，哪些不是。定义交易合法性的规则被写下来后，它们不能自动执行。参与者必须忽略那些不符合规则的交易，而只接受符合规则的交易。

对历史的共识：参与者必须认同比特币经济的历史交易，否则就无法知道谁拥有哪些比特币。

公众对比特币的一个常见误解是，比特币规则一开始就被中本聪敲定了，以后再也不能更改。中本聪确实创建了比特币初始规则集，但它们在任何时候都可以被修改，只要比特币全网达成共识，即比特币社区需要修改该规则。

还有一个误解是，比特币规则可以自动执行，但事实并非如此。比如数字签名，一种数学确定性加密不管是否正确，它并没有自动执行。你随时都可检测到一个不正确的数字签名，但这些不正确数字签名的交易只有在你选择忽略它们时才被默认为无效。

未来，比特币协议可能会为创造更多可扩展性或安全需要而更改。那么，比特币协议怎么实现不断更新呢？

协议更新在技术上是很简单的，比如在源代码中添加一个条件：如果区

块数不超过 200 000，以旧方式执行，否则用新方式执行。

协议更新其实不是一个技术问题，而是一个政治问题，因为更新可能会触犯某些人的利益，比如货币发行速度加快，这可能会遭到大多数人的反对。又比如，若更新没有被广泛接受，那么将出现一个区块链的分叉，失败的一方（通常是采用新规则的区块链）将被忽略。

幸运的是，比特币协议的历次更新都得到了全社区的算力投票通过，通过这些更新，修补了OP_LSHIFT崩溃、无限SigOp DOS、联合输出溢出等多处漏洞。

如果明白上述机制，我们将不难发现，许多对比特币的质疑其实并不成立。比如2013年5月有新闻报道，谷歌参与研制的D-Wave量子计算机的运算速度较配置英特尔芯片的传统计算机快1.1万倍，这让很多人惊呼：比特币已死！因为SHA-256算法很可能会被量子计算机破解。其实SHA-256算法并不是比特币所独有的算法，互联网上大到网银的数字证书，小到USBKey（数字证书）等硬件密钥，使用SHA-256算法的比比皆是。因此，SHA-256算法被破解不仅是比特币的危机，更是整个互联网的灾难。

而且，相对于动则上千台服务器的银行系统，去中心化的比特币对算法破解的应对效率可能会更高效。比特币社区可以按以下步骤应对潜在危机：

在任何人都可以使用新算法之前，预先推广内置新算法的客户端。一旦发生算法破解危机，早期使用新版客户端者（一般情况下是矿池）开始创建新的密钥格式并让区块链接受它们。如果效果很好，标准的客户端将默认为

新密钥。随着时间的推移，最终每个人都同意只能使用新密钥交易，从而淘汰“旧币”。

比特币的护城河在哪里

作为一门技术，比特币会被更高级的技术取代吗？有媒体意味深长地写道：“别再只说比特币了，这儿除了比特币之外，还有你不得不知的其他虚拟货币。”的确，比特币源代码是公开的，谁都可以复制它，修改几个参数，然后宣布创造了自己的货币。目前，市面流行的虚拟货币有莱特币等山寨币，也有硅谷风投所支持的Ripple，还有加拿大皇家制币厂发行的MintChip，它们都或多或少借鉴了比特币去中心化的设计思想。怀疑主义者的疑虑是，比特币的护城河在哪里？

比特币社区有一个共识，即山寨币很难威胁到比特币。以莱特币为例，不同于比特币采用SHA-256算法挖矿，莱特币采用的是Scrypt算法，其计算过程依赖于内存和CPU，使得许多用户用普通电脑就可挖出莱特币，而昂贵的FPGA、ASIC却因内存限制而难有作为，所以莱特币挖矿显得更“环保”（节省算力），也更“公平”。但这只是一种错觉，莱特币挖矿的“环保”是以牺牲安全性为代价的。2013年5月，比特币的全网算力是全球排名前500名超级计算机的总和的8倍，达158THash/s；而莱特币因CPU挖矿的性能限制，全网算力仅为15GHash/s，这意味着后者随时都有被僵尸网络接管的可能。僵尸网络中最多可包含数十万台机器，如暴风木马拥有25万个节点，

假设这些机器的平均性能等同酷睿2双核的算力（5MHash/s），那么暴风木马控制的僵尸网络算力将达到1.25 THash/s，远远超过莱特币的全网算力。又如另外一个自称更“环保”的虚拟货币Freicoin，有好事者仅用两块ASIC芯片就成功地发起了一次51%攻击。

莱特币挖矿的“公平”也是个假象，从理论上说，任何一种挖矿算法都可以为其设计专门的集成电路，这只是个难度问题。事实上，国内已经有人在开发莱特币矿机，他用LX150芯片做一个150M的核，理论速率为60KH/s。莱特币的设计者查尔斯·李也承认：“莱特币刚开始时只有CPU挖矿，一年之后，有人发现也能使用GPU挖矿。一些人认为莱特币比比特币更公平，因为系统还不存在任何集成电路矿机，但这恐怕只是一个时间问题。”

莱特币的拥趸还声称，莱特币每2.5分钟就处理一个区块，而比特币是10分钟处理一个，因而前者的交易确认速度更快。这也是一个误解，对区块链发起一次“双重支付”攻击的进度服从泊松分布，其攻击成功的概率随区块数的增长而呈指数级下降。通过计算不难得出，当区块数大于6个时，攻击成功的概率将下降到忽略不计的程度，这也正是比特币建议6个确认数方可保障交易安全的依据。当区块的处理速度提高至比特币的4倍时，攻击者制造出一个假节点的成功概率也急剧上升，通过计算泊松分布的概率密度，避免双重支付攻击所需要的节点确认数也将上升至比特币的4倍，即莱特币需要24个节点确认才能达到比特币6个节点确认的安全性。

比特币堆积庞大算力、消耗巨大能源，其目的却是解一堆毫无意义的数

学题，这一设计思想一直饱受批评。马克·吉梅恩在彭博社发文称，比特币采矿创造了现实世界的环境灾难。他指出，比特币每天采矿需要耗费98.2万度电，足以为3.1万美国家庭供电，是大强子对撞机所需电力的一半。在《纽约时报》的专栏文章中，保罗·克鲁格曼引用亚当·斯密的话称："金银货币最愚蠢的地方是它们的功能是象征性的，但在生产中却需要消耗真实的资源，用纸币取代它们是明智之举。虽然现在是信息技术时代，但比特币却在复制亚当·斯密于18世纪所说的愚蠢。"就连比特币的支持者也不甚了解这一设计思想。米塞斯圈的一位专栏作者撰文称，比特币穷兵黩武地堆积算力，跟孔雀进化出华丽的尾巴、爱尔兰大鹿进化出3.6米的大角一样，是囚徒博弈的最佳选择，这在生物学上叫作累赘原理[①]。这种解读当然很无厘头，与比特币"计算即权力"的设计思想相去甚远。

既然比特币网络拥有堪称人类有史以来最大的算力集合，为何不把这些算力用于蛋白质折叠、寻找外星人、寻找素数等功在千秋的科学计算呢？素数币便是这样一个自称"非能源效率"的山寨币，它企图将算力用做寻找素数的科学计算。它的发明人雄心勃勃地写道，"加密货币目前已经分道扬镳为两条道路，一种是能源密集型，一种是环保节能型。我相信，在未来较长一段时间内（5年以上），环保节能型货币将因其成本优势而开始挑战能源密集型货币。素数币第一次引入非哈希现金的工作量证明机制，使得算力不仅仅用来制造区块链，还提供额外的潜在科学价值。"

① 累赘原理，由以色列生物学家扎哈维提出，指一桩事可能因为它有危险而能够带来更大的机遇。

很遗憾，既要用算力来保障P2P货币安全性，又要用算力来做有用的科学计算，这是一个二律背反。比特币社区的计算机工程师认为，把“难度可调”的NP难度问题（比如SHA-256算法）嵌入蛋白质折叠算法是可能的，使计算蛋白质折叠问题成为挖矿的一个副产品。挖矿除了生产货币之外，还能产生社会效益。但这种貌似“有用的”的工作量证明算法实际上会对区块链的安全性构成威胁。试想一下，使用比特币挖矿算法来进行蛋白质折叠、寻找外星人、寻找素数等分布式计算，比特币的安全性根基（没有任何节点可以控制全网大部分算力）就崩溃了。因为分布式计算的工作量是可叠加的，随着工作量证明功能的“有用部分”的增长，攻击成功的可能性也在增长。即使你一个区块也没找到，你完成的工作量仍然对别人有用，黑客可利用你完成的这部分工作量降低网络攻击的成本。所以，理想的设计是矿工完成的工作量对其他人来说是无用的，这样才能保证他们扔掉的计算量是一个与硬件成本、电力、运气或带宽有关的商品。

为此，素数币做了一定改进，设计了一个非可重用性的工作量证书，即一个区块上的工作量证书不能用于其他区块。为实现此点，它将素数链连接到的区块头哈希除以父级区块头的哈希所得的商作为工作量证书。工作量证书与区块的哈希值一同嵌入子区块中，这样不仅能够防止工作量证书被篡改，同时可以避免产生一个可在多个区块上重复使用的工作量证书。这种改进的效果是，将一万个人同时挖一个坑的游戏变成了一万个人同时挖一万个坑的游戏，任何人完成的寻找素数工作量都只能为己所用，素数币的计算资

源并未用于分布式计算，计算成果未能实现全网共享，计算负载也未能在节点中平衡。可见，它本质上仍然是一种能源密集型货币，与它“非能源效率”的设计初衷相悖。

还有一个严重的问题是，素数在数轴上的分布是不均匀的，位数越大则越稀少，寻找难度呈指数增长，工作量证明却需要难度平滑增长。这意味着越到后面，素数币的交易越难确认，甚至不能确认。素数币的解决方案是用一种费马测试的改进版进行素性测试，这样可以提高效率，节省计算时间，但这是一种不完备的筛选，因为费马测试是基于费马小定理的逆定理，而该定理已经被证明不成立，费马素性测试得到的是伪素数，素数币寻找到的坎宁安链越到后面越不可信，其寻找素数的所谓“潜在科学价值”恐怕也只能停留在“潜在”这一步了。

一些人将山寨币之于比特币的关系，视作其他贵金属之于黄金的关系，比如莱特币就用心良苦地把货币总量设计为比特币的 4 倍，企图像白银锚住黄金价格一样，锚住比特币的汇率。莱特币的推广词就是：如果说比特币是数字金币，那么莱特币就是数字银币。还有羽毛币把货币总量设计为莱特币的 4 倍，试图成为数字铜币。这种想法似乎过于一厢情愿了，因为元素周期表上的元素终究是有限的，而山寨币却可无穷复制，层出不穷的模仿者最终只能稀释所有模仿者的价值。自 2013 年 5 月以来，社区以每天两三种的速度发布新的山寨币，几乎所有山寨币都呈下跌走势，虚拟货币 PPcoin 从最高的 0.003 比特币跌到 0.001 4 比特币，虚拟货币 Yacoin 从最高 0.000 6 比特币跌到 0.000 15

比特币，还有更多的不知名山寨币走向价值归零或退市的穷途末路。

就目前市面上出现的山寨币或其他虚拟货币来看，尚未发现有价值的技术创新。其实，就算后来者涌现出突破性的技术创新，比特币社区也很容易就能加以借鉴，将之添加至比特币核心协议，并升级客户端。“没有护城河，才是终极护城河。”一个比特币迷在微博上如是说。比特币是像车轮一样的发明，重复发明轮子是徒劳无益的，因为世界本质上只需要一种数字货币。但山寨币的存在并不是毫无意义，它的存在有助于比特币的自身进化。由于比特币生态已经蔚为大观，社区对每次可能导致“硬分岔”的协议升级都非常慎重，山寨币则可以充当小白鼠。比如，彩色币、零币等应用可以率先添加进莱特币等山寨币的协议，如果获得成功，转而应用于比特币中，这将大大降低协议升级、软件更新所带来的“硬分岔”风险。

比特币会内部崩溃吗

与传统的层次分明的金字塔组织方式不同，比特币因其去中心化的P2P网络结构而开启了一种开放式的信息组织与进化模式：没有命令，只有很弱的组织，相当于蚂蚁筑巢。比特币社区继承了开源社区的传统，用倾听取代强权，用沟通取代命令，用协商取代控制。比特币社区唯一官方意义的组织是比特币基金会，仿照Linux（一种开源的操作系统）基金会的模式建立，依靠用户捐助的比特币维持运营，负责组织比特币核心协议的完善、客户端的升级、安全性的监督、法律事务以及与政府机构的接触等。

比特币社区也不存在真正意义上的领袖，加文·安德烈森被视作中本聪的继承者，他是比特币社区的仲裁者和架构师，同时负责协调比特币核心程序的优化。安德烈森成为比特币社区领导者的过程非常简单。起初他向中本聪提交优化比特币核心系统的代码，中本聪逐渐对他的代码有了信任。有一天，中本聪问他是否可以将其邮箱地址放在比特币的主页上，安德烈森同意了。从此，比特币主页上中本聪的邮箱地址被安德烈森的邮箱地址取代，项目的领导者象征性地过渡给了安德烈森，中本聪则退到了幕后，甚至消失了。中本聪与安德烈森都不能对比特币社区发号施令，与普通开发者的唯一区别是，他们拥有一个可以在客户端添加警报的密钥。

比特币社区信奉海盗式的民主，每个节点都可用自己的算力进行投票，任何针对客户端的改进、协议的修改与添加都将置于算力投票的监督范畴内，只有被全网51%以上的算力接受的改进才能真正视作有效。与海盗社会一样，差劲的领导者很快就会被社区抛弃。历史上曾有一伙海盗在某趟航程中更换了13个船长，其中有个叫本杰明·霍尼戈的船长，手下们罢免他的原因居然是他“拒绝攻打和劫掠英国船只”。试想一下，若比特币社区真的存在一个为所欲为的“船长”，比如安德烈森在客户端里加入某种后门程序，可以让他轻易地挖到比特币，或者他独断专行，执意推行被社区多数人反对的协议升级，那么用户完全可以无视其发布的程序，采用社区其他程序开发者的程序交易比特币或挖矿即可。

中本聪认为，20世纪90年代以来，Beenz、Flooz等虚拟货币先驱的失

败主要是由其中心化的组织结构造成的。其主要原因是，一旦为虚拟货币信用背书的公司倒闭，或保管总账的中央服务器被黑客攻破，该虚拟货币就将面临信用破产与内部崩溃的风险。所以，他将比特币设计为全分布式拓扑结构，这也是人类历史上第一次尝试去中心化、不再依赖对中央发行机构的信任的货币系统。一般认为，全分布式拓扑结构具有良好的可扩展性、鲁棒性和自组织性，像蚂蚁社会一样，拥有不可思议的自我修复能力。

科幻小说《马姨》构思了这样一个故事情节：有人用蚁群设计了一个自组织的机器智能“马姨”，以蚂蚁个体的本能行为执行计算机指令，并通过代码手册与人进行交流，在整体上表现出一定的机器智能。主人公从蚁群中赶走一些个体，但惊奇地发现“马姨”的运行一切正常。

比特币就是这样一个具有强鲁棒性的系统，每时每刻都有大量节点频繁地加入或退出，但丝毫不影响全局结构的稳定性。比特币社区里有人打趣道：“这就好比在诺克斯堡[①]周围每隔 10 英尺安排一个武装狙击手，仅仅是用来保护一袋分币钢镚儿。让这些狙击手一半回家休息，这袋钢镚儿的安全性丝毫不会降低。”

同样，从技术上关闭比特币相当困难。2009 年 2 月，中本聪在IRC（互联网中继聊天）频道写道：“政府擅长击溃Napster（一种在线音乐服务）那样拥有中央控制的网络，但是Gnutella 和Tor 这样完全P2P的网络看起来依旧安枕无忧。”

① 诺克斯堡，一个位于美国肯塔基州的装甲师训练基地。

值得一提的是，另一个自称分布式的虚拟货币Ripple在网络结构上与比特币有着本质的区别。比特币网络结构符合随机网络特征，节点连接是随机的，大部分节点的连接数目大致相同，即节点的分布方式遵循钟形的泊松分布，存在一个特征性的“平均数”。连接数比平均数高许多或低许多的节点都极少，随着连接数的增大，其概率呈指数级迅速递减。而Ripple网络更类似于无尺度网络[①]，它引入“共识”机制，通过特殊节点的投票对交易进行验证和确认。而这些特殊节点往往拥有大量的连接，大部分普通节点的连接数却很少，节点连接数符合齐普夫定律[②]。这种特殊节点的存在使得Ripple网络对意外故障有强大的承受能力，但面对协同性攻击时则十分脆弱。研究表明，面对蓄意的协同攻击时，只要5%~10%的集散节点（拥有大量连接的节点）被移除，无尺度网络就将彻底瘫痪。

更糟糕的是，Ripple客户端为加快确认速度，不需要下载区块链，而是在普通节点上舍弃已经验证过的总账本链，只保留最近的已验证总账本和一个指向历史总账本的链接，显然，那些保管历史总账本的服务器就成了它的软肋。

尽管Opencoin公司小心地隐藏了服务器端源代码，但对于黑客来说，找到通往服务器之门并不是一个技术问题，而是一个经济学问题。随着Ripple网络的交易额逐渐上升，黑客对它的欲望也越来越强烈。2013年6月，Ripple连续发生多起在线钱包失窃事件，虽然这些失窃可能都是用户密

① 无尺度网络是指由少数一些具有众多连接的节点支配的网络。

② 1932年，哈佛大学的语言学家齐普夫发现，语言中每个单词出现的频率与它的排名的常数次幂存在简单的反比关系，只有极少数的词被经常使用，而绝大多数词很少被使用，这种分布就叫作齐普夫定律。

码设置的疏忽所致，而不是来自系统攻击，但这也表明，一大波黑客正在向Ripple袭来。7月，Ripple平台遭遇分布式拒绝服务攻击，黑客从一个账号向另外一个账号发起大量小额转账操作，让Ripple平台的服务器无法响应和支撑其他用户正常的交易请求，造成Ripple服务中断长达十几个小时。

可见，在抗攻击问题上，Ripple与过去的Beenz、Flooz等虚拟货币以及“自由美元”等私铸货币并无本质上的不同，这也难怪一个资深用户讽刺Ripple说，疯子就是一遍一遍做同样的事，却期待不同的结果。

但是，既然比特币出于安全性、健壮性考虑，致力于建设去中心化的全分布式结构，中本聪为什么亲自设计了中心化的矿池呢？目前，BTCGuild、50BTC、ASICMiner三大矿池已经占据全网64%的算力，这意味着三大矿池若联手，将足以对比特币网络发起51%攻击。黑客丹·卡明斯基在2013年比特币大会上表示，比特币网络存在系统性风险。反对者却认为，矿池的存在是对比特币安全性的增强。

矿池对比特币网络的组织有什么作用呢？凯文·凯利在《技术元素》一书里提出了一个思想：“只从底部出发还不够。”即使是互联网最大的开放性自组织工程维基百科，也不是完全自下而上的组织形式。维基百科的维护者设计了严密的条框来防止网络小白任意修改词条，超级管理员可以采用精英编辑的建议单方面屏蔽他们。凯文·凯利认为，在网络经济中，真正的商业和组织艺术不在于控制包括“每个节点”的群体，而是在最佳时间为每一个利基市场找到底层和顶层的最佳组织。矿池的存在可以让比特币网络对安全

预警、漏洞修复的反应更敏感和高效。

2013 年 3 月，比特币 0.7 版和 0.8 版客户端因区块大小限制的不同而导致不兼容，互不承认对方的有效性，比特币网络面临分裂的危险局面。比特币社区发出警报之后，几大矿池迅速响应社区的呼吁，将客户端切换到了旧版本，仅用了几个小时便化解了这次危机。试想一下，若没有矿池的存在，全网几百万个节点需要在短时间内同时切换客户端才能避免这一危机，这恐怕是不现实的。

在比特币的工作量证明机制中，算力即投票权，算力越大，权力越大，责任也就越大。所以，在比特币基金会的成员名单上，你看到各大矿池的管理者的名字也就不足为奇了。中本聪认为，如果是用节点数即IP地址的多少来决定谁是大多数，那么拥有分配大量IP地址权力的人，比如僵尸网络，就有可能主宰比特币网络。而工作量证明机制的本质是一CPU一票——计算即权力。拥有更高算力的人更有责任保障全网的安全，因为比特币的挖矿激励机制使得在非合作博弈中存在一个纳什均衡，即把算力用于诚实挖矿较用于发起双重支付攻击获得的回报更高。

2013 年 4 月，BTCGuild矿池的算力份额一度接近全网的一半，引发了社区对 51%攻击的担忧。为此，BTCGuild的管理员Eleuthria（网名）主动限制了算力的增长，规定如果矿池算力超过了 45%，将移除所有基于getwork协议（一种直接连接到矿池挖矿的协议）的服务器，并关闭新用户注册，直到算力回到 40%以下。

矿池拥有者杜绝51%攻击的意愿比普通用户更强，Eleuthria在社区发帖说："显然，我不能等到矿池算力份额到了49.9%时才采取措施，即使51%攻击只有在控制它的人决定这样做时才会发生。"一个理性的决策者绝对不会把可兑现成真金白银的算力用来发起回报有限的51%攻击。退一步说，即使部分矿池拥有者是疯子，他们无视利益的大小，执意对比特币网络发起攻击，比特币社区发出警报之后，矿池用户只需停止运行矿机或切换至普通方式挖矿，便可让疯狂矿池的阴谋落空。毕竟矿池只是承担计算任务分发与挖矿奖励分配的平台，而不是矿机的真正拥有者。

比特币会成为标准吗

如果说开源操作系统Linux就像芬兰史诗《卡勒瓦拉》那样不断完善，由最初的约1 000行代码，经黑客社区的义务贡献，成长为目前规模达100万行的庞大系统，那么，今天的比特币正沿袭这条英雄史诗之路，像远古的巨茎植物一样不断向天空生长。在过去的3年中，共有120多位程序员为Bitcoin-QT提交了5 000多次代码改进，为比特币开发应用程序与网站的程序员更是逾千。比特币核心协议在不断地自我完善，而零币、彩色币、域名币、分布式合同、智能资产等新的拓展协议也试图添加进比特币核心代码，或在比特币协议基础之上构建延伸至其他领域的应用。这是一座真正的通天塔！

传说巴比伦塔直插云霄，希望通往天堂。上帝为之震怒，为惩罚这些

狂妄的人，便让建筑巴比伦塔的人们使用不同的语言，因语言的不通，还没完工的巴比伦塔很快就被废弃了。也许未来货币也将面临同样的问题，比特币越来越像是一个开放式的基础平台，但它会成为虚拟货币世界的通用语言吗？

如前所述，比特币提供了3个层次的开放性，使货币与金融成为程序员施展创造才华的天堂，以比特币为基础平台，可提供数不胜数的更高层次的服务，例如资金混合、货币兑换、财务管理与预警、市场数据分析、计量服务等。如果将比特币视作互联网的IP协议，那么就不单会有类似TCP的API和协议扩展，还会有在此之上的协议层提供的各种服务，类似互联网的SMTP、HTTP等应用层协议。比如利用底层的分布式总账，开发者推出了存在性证明、期货合约、数字版权等应用。正如Group合伙人安德烈亚斯所言："货币作为一项服务，通过开放的、灵活的、强大的API构成一个完整的经济体系，一切都只是一个JSON（一种轻量级的数据交换格式）请求。如果你认为比特币只是电子货币，那么你只看到了冰山一角。"

互联网协议的发展有很强的路径依赖特性，一旦选择进入某一路径，哪怕该路径具有某种缺陷，也会对这种路径产生依赖。

美国铁轨的故事[①]有助于我们理解这一概念。美国铁路两条铁轨之间的标准距离是4.85英尺（约合1.5米），为什么是这个尺度而不是别的什么尺

① 有人指出，铁轨路径依赖的故事尚存争议，因为世界上存在各种铁轨标准，古罗马的道路主要走的不是马车，而是人力推车。但路径依赖现象在社会生活中很常见，一项制度一旦走上某条发展路径，就会在以后的发展中自我强化，并一直沿用下去。

度呢？原来这是英国的铁路标准，而美国的铁路最早是由英国人设计建造的。那么，为什么英国人采用这个标准呢？原来英国的铁路是参考电车轨道设计的，而4.85英尺正是电车轨道的标准。追溯电车轨道的标准，我们会发现，原来最早制造电车的人是以马车的轮宽为标准的。那么，马车的轮距为何这么宽呢？这是因为英国的旧马路上布满了这个宽度的辙痕，如果用其他轮距的话，马车的轮子很快就会磨坏。为什么旧马路上会有4.85英尺宽的辙痕呢？答案是，这是古罗马人留下的，4.85英尺正是罗马战车的宽度。罗马人为什么用4.85英尺作为战车的轮距宽度呢？原因很简单，这是两匹拉战车的马的屁股的宽度。

路径依赖的故事时至今日仍没完，下次你在电视上看到美国梭立在发射台上的航天飞机雄姿时，注意观察一下燃料箱两旁的两个火箭推进器，这些推进器是由犹他州的工厂提供的。如果可能的话，这家工厂的工程师希望把这些推进器造得再大一些，这样容量就会更大，运输更经济，但是他们并没有这样做，为什么？因为这些推进器造好后，要用火车从工厂运到发射点，路上要通过一些隧道，而这些隧道的宽度只比火车轨道的宽度宽了一点点。因此我们说：今天世界上最先进的运输系统的设计，其实是2 000年前便由两匹马的屁股宽度决定的。这说法看似荒谬好笑，但却也站得住脚。

随着互联网的爆炸式增长，新的协议特别是高层应用协议在不断涌现，而互联网核心通信协议TCP/IP竟然已存在了30多年，这在瞬息万变的信息技术世界堪称奇迹。但按照路径依赖原理，这完全是合乎逻辑的。在单机上，

人们可以很容易替代很多计算机技术，然而网络协议的更换并不是那么简单，它要求整个网络的所有设备都进行更新，这也是IPv4（网协版 4）面对地址耗尽的压力仍能长期存活的原因之一。有一些网络协议的设置在今天看来很笨拙，但在当时是聪明的解决方案，而后来的协议必须兼顾之前已有的协议。

合并挖矿的实现，使域名币、彩色币等其他应用的区块链并入到比特币网络中，恰如新建的铁轨采用同样制式并入到已有的铁轨网络一样，是一个路径依赖的过程。不难想象，当域名币、彩色币、分布式合同等应用得到推广，建立于其上的相关应用亦必将沿用比特币的区块链。莱特币等山寨币如雨后春笋般冒出来，但它们很难吸引到追随者为其完善代码和开发应用。更何况比特币矿池的设计使比特币协议的自我更新效率远远高于传统互联网协议，这让莱特币等后来者难以追上比特币的步伐，取而代之则更是难上加难。

为什么数学比人可靠

/数字让世界更守信/

比特币常被人诟病的一点就是，没有人能为它的信用背书，缺乏一个让人信赖的权力机构来保障比特币的安全与价值，如果比特币崩盘，用户只能自己承担损失。比特币支持者的观点则恰好相反，他们认为，正因为在比特币的系统中不存在货币发行机构和交易担保，而只有严密的数学算法，它才是最安全的，因为数学是诚实可靠的。其他使用工作量证明机制的P2P货币能击败比特币吗？答案是，不可能，因为在其算力追上比特币之前，它已经

被比特币网络的算力攻陷了。这就好比一个说法：没有人能击败逻辑，因为要击败逻辑，你还得使用逻辑。

文克莱沃斯兄弟对此颇有感触："我们已经决定将我们的钱和信仰投入到一个数学框架中，它不会被政治和人类愚蠢的错误干扰。"当时，人们已经知道他们大约拥有已生产的比特币总数的1%（90 000多个比特币），其比特币大亨的身份难免让人怀疑其吹捧比特币的动机，但他们只是在阐明一个事实而已。文克莱沃斯兄弟确实应该相信数学，如果比特币早些问世，他们也就用不着与扎克伯格打一场长达3年的官司，因为他们可以利用比特币"存在性证明"功能，轻易地证明自己才是Facebook创意的最初拥有者。

比特币确实能让世界变得更诚信、更有序、更美好，它的存在性证明、零知识有条件付款、分布式合同、智能资产等应用都无须担保中介的介入，仅用密码学原理和呼叫应答广播机制便能让欺诈无处遁形，让怀疑论者无从置喙。

/比特币密码学的可靠性/

支付宝、财付通、网银等传统电子支付工具以邮箱地址、QQ号码、银行卡号作为用户ID，用户稍有疏忽，就可能将钱打入别人的账户。在比特币世界，这样的事绝对不可能发生。比特币的地址是一串无意义的数字，用户在拷贝或输入这串数字时，无论出现何种错漏，都不会将钱误转入别人的账户。比特币地址由33位Base58编码的数字或字母组成，可用的比特币地址理论上超过2^{160}个，全世界约有2^{63}粒沙，比特币地址总数远远超过地球上

所有沙的数量。错误输入的比特币地址恰好是别人的比特币地址的概率，比飞入你眼中的一粒沙恰好是去年你在沙滩上踩到的一粒沙的概率小得多。

虽然MD5、SHA-1算法的安全性根基已被动摇，但就目前而言，比特币所使用的SHA-256算法仍是可靠的，美国国家标准技术研究院就建议原来使用MD5、SHA-1算法的安全系统都切换到SHA-256算法。而且，作为电子支付手段，比特币未雨绸缪，它并不直接使用公钥作为比特币地址，而是在公钥的基础上再散列两次，人们一度质疑这只带来了不必要的麻烦和浪费。但事实证明，中本聪是对的。因为量子计算机可以破解椭圆曲线数字签名算法，但它们仍不足以逆转哈希算法，这需要花掉2^{80}个步骤来完成一个比特币地址的破解，如果你的比特币资金存放在一个没有公开过的地址，它们在量子计算机面前仍是安全的。

但到了今年9月的时候，又一则爆炸性新闻的曝光让比特币安全性再次面临威胁，据英国《卫报》报道，一家美国主流计算机安全公司已告知数千名用户，立即停止使用一个由美国国家安全局（NSA）开发的加密标准。这一警告发出前不久，美国前中情局雇员爱德华·斯诺登披露了NSA监控项目，称NSA采用秘密方法控制信息安全国际标准的制定，这一标准由美国国家标准技术研究所（NIST）运行，因此其可以被NSA破解，而比特币采用的椭圆曲线算法正在其列。漏洞在于椭圆曲线算法的两个参数是由某个种子经哈希算法生成，而这个种子正是国安局精心选择的，他们可以采取不为人知的方法来弱化这条曲线。FBI得知这一消息可能会欣喜若狂，因为他们正

为破解乌布利希的私钥绞尽脑汁。但是很遗憾，比特币让他们失望了，中本聪使用的不是伪随机曲线，而是Koblitz曲线，如果是前者，NSA则有可能找到一条特定曲线的椭圆函数的漏洞。高效密码学组标准的现任主席丹·布朗得知比特币使用的是secp256k1时也深感震惊，因为只有极少数程序躲过了这一潜在灾难，比特币便是其中之一，中本聪的前瞻能力可见一斑。

在《技术元素》一书中，凯文·凯利虽然承认“比特币技术令人惊讶，复杂到几乎超越大部分外行用户的理解范围”，但他也认为，“通常来说，加密方式没有被直接破解的，都是通过使用方式被间接破解的。只要出钱足够多，任何东西都可以被黑客黑掉。”凯文·凯利怀疑的后半句有待商榷，如果你拥有比特币全网一半以上的算力，或者你能破解SHA-256，你的确能够黑掉比特币，很可惜，这两件事都不是给钱多就能办成的。但他的前半句点出了要害，加密很少从数学上直接破解，多数是从用户那里打开缺口。

以拖库攻击为例，在口令保存上使用最广泛的算法是标准MD5。MD5算法具有不可逆的特点，即不可能从明文得到用户口令。但其不可逆的前提是，假设明文集合是无限大的，而用户设置的口令却是一个具有高度统计规律的有限集。因此，攻击者很容易通过“密文比对+高频统计”的方法生成密文字典，再通过对照密文字典或彩虹表一举攻陷MD5加密的口令。在这个过程中，MD5算法本身是可靠的，漏洞出在用户设置口令的规律性上。

一个安全系统中最薄弱的环节往往不是算法，而是人类。而比特币的设计从一开始就排除了人的参与，地址的生成、挖矿算法的“掺盐”都是自动

的、随机的、匿名的，天生对社会工程学攻击和彩虹表攻击免疫，无论在哪个环节，都不存在统计上的规律性。著名黑客丹·卡明斯基曾花了两年时间尝试攻击比特币，但他失败了。他在博客上写道："比特币让我吃惊，它是这样一个系统：创造了一个巨大的全球云，始终保持在线接听状态，通过烦琐细致的自定义网络协议保持通信。"

/革命性的前景/

比特币优雅的数学内核刚一问世就得到了计算机界的高度赞赏：电子现金系统B-Money（B钱）发明人戴伟认为比特币的发明"意义重大"；尼克·萨博称赞比特币是"对世界的伟大贡献"；著名密码破译专家哈尔·芬尼称它"具有改变世界的潜力"；创业公司OnlyOneTV的布鲁斯·瓦格纳称其为"自互联网问世以来最令人激动的一项技术"。

硬币的另一面却是另外一种景象：诺贝尔经济学奖得主保罗·克鲁格曼将比特币定义为"金色的网络桎梏"；职业经理人唐骏在财经节目中称"比特币啥也不是"。缘何汝之蜜糖，却是彼之毒药呢？

福布斯专栏作家蒂莫西·李以公众对非对称加密技术的态度为例来解释这一现象。程序员与非程序员第一次听到比特币时的反应截然不同，程序员对比特币普遍比较兴奋，而其他人却是不以为然。许多人从一开始对比特币持怀疑态度，但其怀疑的性质是不同的。非程序员根本看不出这里面有什么值得大惊小怪的成就，他们以为比特币与传统的支付系统只有细微的区别，

而程序员则相反，他们立即看到了比特币具有的革命性前景，它只是需要时间去说服公众。

比特币从理论构建到技术实现，历经戴维·乔姆等杰出程序员数十年的技术接力，才由中本聪最终完成达阵。它允许财富以纯信息、零成本的形式发送给全世界任何人——这在2009年之前人们是闻所未闻的。它将不会立刻显示出效果，尤其是对普通用户来说。但是，就像非对称加密技术一样，它若干年后将被证明是与交流电一样伟大的发明。

结语
年轻、疯狂和自由

2013 年 5 月，我和长铗商量写一本关于比特币的书，之后我们各自的朋友陆续加入。在写这本书之前，我们在现实中素未谋面，甚至观点迥异，但这并不妨碍我们彼此信任，以开源社区的方式共同创作。我们可能是国内最早关注和参与比特币实践的群体，也在努力传播比特币的思想。我们翻译了大量技术论文、与虚拟货币相关的报告，传播去中心化自由货币的理念，只希望在我们和你之间建立共同的资料基础，并认真思考比特币及其思想。

我们凭着热情和笃信，学习哈希算法和非对称加密，阅读奥地利学派和货币理论，重拾让人抓狂的英语文献。当然，我们也都参与了比特币的实践——挖矿、交易、支付、传播、衍生市场等。比特币不仅是一种金融工具，更是一种生活方式和思想理念，真实地改变了我们的生活轨迹。就像长铗说的：20 岁之前，我还能被第一推动、太空、量子论之类的科技名词鼓舞；20 岁之后，我发现，与其在文字中构思那些未来的场景，不如亲自投身于一项足以改变世界的技术或思想，无论结果如何，这一过程着实美妙。

在这样的想法下，长铗建立了比特币中文社区巴比特，是重要的比特币

思想传播阵地。我和我的朋友“七彩神仙鱼”、“暴走恭亲王”合作成立了“壹比特数字科技”，从事数字货币的资讯传播、数据挖掘和工具研发等，希望能为行业生态建设贡献力量。两位伙伴有着神奇的网名，性格迥异、年纪不等，是互联网普惠平等的思想和去中心化的理念让我们走到了一起。

比特币能否改变世界呢？假如衡量标准是比特币是否在短期内替代法币，那我认为其结果是不能的。但是，比特币仅仅是一种货币吗？我觉得也不是，也不该是——可能改变世界的是比特币的技术和思想，而不局限在货币的范围内。把比特币仅仅看作一种货币，而不是一种革命性的思想或一整套交易架构和生态，那显然是小看了比特币。即使把它的影响限定在更广的金融领域，也未必是合适和恰如其分的。这一点，相信你在阅读中也会发现。

发轫于思想，不拘于形态。我从不笃信某种形态和表现，相信的只是原则和思想。对于狂热的比特币信徒来说，比特币的未来就像数学公式那样清晰明了。他们甚至排斥“信徒”的定义，因为数学不是一种信仰，而是一种认识论。而对我来说，信便能，不信便不能，就像新教伦理里面讲到的因信称义。我们只是尝试搭建一个让大家足够相信的逻辑基础——当然，最符合逻辑的不一定是最终存活的。

比特币之于我们的吸引力，正如20世纪50年代实验室里的巨型机对麻省理工学子的冲击，70年代车库里的微型机对辍学大学生们所释放的魔力，这种毫无来由的沉迷有一个共同特点，那就是他们都奉行与计算机本身雅致的逻辑相一致的理念——开放、平等、协作、分享，以及不惜一切代价亲自

动手改进机器并改善整个世界。这种理念本身是年轻、不羁与自由的，抱着对世界的诚恳与善意。年轻、疯狂和自由，这足以让我们不遗余力地推动比特币的发展。

比特币是一个新事物，大家对它的看法也不尽一致。本书无意表达绝对正确的观点，而只在于展示一种新思想，它或许是一种潜在的未来，或是一个玩笑，或者什么也不是。这应该是全球关于比特币的第一本书，我们也尽可能讨论比特币的所有重要内容，并形成相对系统性的论述。

最后，感谢朱嘉明老师分享他的观点，以及对我的信任和帮助。感谢李笑来老师倾情作序。感谢比特币基金会成员的真诚推荐。感谢耀东老师在全书统稿和修改过程中做出的重要贡献。

李钧

壹比特数字科技首席执行官

货币的自发演变被国家对货币的垄断中断。信息技术和互联网是否会改变国家对货币的垄断？这本书将引导你思考这个问题。

张维迎
北京大学光华管理学院教授

比特币的技术和思想可能是过去十年里互联网行业的最大创新。这本书揭示了比特币的历史、科技和未来，将为比特币的发展做出重要贡献。

曹大容
光速创投合伙人

这是一本关于未来货币的书。极客们犹如在演习新的魔法，憋足劲准备叫人大开眼界，这事酷极了——哪怕谁也无法担保成功。

姬十三
果壳网首席执行官

两年后（也许用不了那么久），比特币还会冲破一个在此之前被认为是疯狂的价格，然后再引来一轮更大的关注。

李笑来
资深比特币投资人

上架建议◎经济读物
ISBN 978-7-5086-4300
9 787508 643007 >
定价：39.00元